

N°52

Casser les codes et décrypter l'info



Avril / Juin 2022

PIRATE

INFORMATIQUE

HACKING
REVEALER,
le **KEYLOGGER**
qui frappe fort



VIE PRIVÉE

7 Alternatives
LIBRES POUR
QUITTER
GOOGLE

HACKING
de **A à Z**

GUIDE COMPLET

PILOTEZ VOTRE
SAUVEGARDE
AVEC **FBACKUP**

✂ **100 % GRATUITS**

✂ **Tests, Tutos & Astuces**

TOP 5
LOGICIELS de
MONTAGE VIDÉO
GRATUITS



BLACK DOSSIER

CYBERGUERRE
Résister à
l'**OGRE RUSSE**





SOMMAIRE

BLACK DOSSIER

11-21

RÉSISTER À L'OGRE RUSSE

LES LEÇONS D'UNE CYBERGUERRE



HACKING

22-23

> Surveillez chaque mot grâce à un **KEYLOGGER**

24-25

> Analysez votre **CONFIGURATION PC** avec **AIDA64**

26-27

> **ASPIREZ** tous les **EMAILS** d'un site Web

28

> Gardez votre **HISTORIQUE** en navigation privée
> Générez des emails à **USAGE UNIQUE**

29-31

> **HOVERWATCH** : Mais que fait la police ?



32

> **MICRO-FICHES**

ANONYMAT

34-37

> **TOP 7 ALTERNATIVES** pour virer **GOOGLE** !

38-39

> **CLÉ USB** de secours : un **ANTIVIRUS** à portée de main

40-41

> **PIXELS ESPIONS** : Quand vos mails vous espionnent

42

> **MICRO-FICHES**



SOUTENEZ-NOUS !

Vous découvrez ce magazine en l'ayant téléchargé illégalement ? C'est de bonne guerre, nous sommes pour le partage ! Merci de l'intérêt que vous portez à nos articles, mais pour que nous puissions continuer l'aventure, pensez à acheter le magazine : offrez-le, parlez-en autour de vous ! *Pirate Informatique* existe depuis plus de 10 ans, sans publicité et sans hausse de prix !

PROTECTION

44-47

> Comment détecter et se protéger des **SITES FRAUDULEUX** ?

48-52

> **GUIDE COMPLET : SAUVEGARDE** facile et automatisée avec **FBACKUP**



53

> **MICRO-FICHES**

MULTIMÉDIA

54-55

> **TOP 5 MONTAGE VIDÉO**

56-57

> Trouvez et écoutez des **PODCASTS**



58

> **PROXYFREE** : Contournez les limitations de pays

59

> **TÉLÉCHARGEZ** du contenu d'**INSTAGRAM**
> **ÉLIMINEZ** un élément gênant d'une **PHOTO**

60

> **MICRO-FICHES**

62-63 > NOTRE
SÉLECTION DE MATÉRIELS

Avril / Juin 2022

Une publication du groupe ID Presse
Impasse de l'Espéron - Villa Miramar
13960 Sausset Les Pins

Directeur de la publication :
David Côme

Rédacteurs :
Fabrice Brochain, Mélanie De Coster

Maquettistes : Sergei Afanasiuk
et Stéphanie Compain

Correctrice : Marie-Line Bailleul

Service Abonnement :
Indiquez la référence *Pirate Informatique*
dans vos échanges
Tél. : 03 44 51 97 21
Email : abonnement.bii@gmail.com

Imprimé en France par
/ Printed in France by :

Mordacq Impression
Rue de Constantinople
62120 Aire-sur-la-Lys
France

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : 0722 K 94236

ISSN : 1969 - 8631

«Pirate Informatique»
est édité par SARL ID Presse,
RCS Aix-En-Provence 491 497 665

Parution : 4 numéros par an.

La reproduction, même partielle, des articles et illustrations parues dans «Pirate Informatique» est interdite. Copyrights et tous droits réservés ID Presse. La rédaction n'est pas responsable des textes et photos communiqués. Sauf accord particulier, les manuscrits, photos et dessins adressés à la rédaction ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.



LIGNES DE FRONT

À l'heure où nous écrivons ces lignes (début mars), impossible de connaître - ou ne serait-ce qu'imaginer - l'évolution à venir du conflit russo-ukrainien. Pour autant, après 15 jours de guerre, de nombreuses leçons inattendues sont venues redéfinir notre perception et nos connaissances sur l'arsenal cyber russe. Et nous donner aussi de nombreuses pistes sur la façon de résister à ses ambitions déstabilisatrices ou mafieuses. Notre dossier dresse un panorama des différentes lignes de front numériques qui se sont établies, côté ukrainien, russe et international.

N'oubliez pas que la connaissance et l'accès aux outils informatiques libres sont des armes. La liberté dont nous bénéficions aujourd'hui dans nos sociétés occidentales est un moment rare de l'histoire. Il n'est pas dit qu'il dure longtemps. Alors ne vous endormissez pas, continuez d'être exigeants et restez pirates dans l'âme.

La rédaction



CYBERASSURANCES : LE RISQUE D'UNE DÉSERTION

Generali vient d'annoncer ne plus assurer les rançons de cyberattaques payées par les entreprises. L'État français demande désormais aux clients et assureurs de développer des contrats très pointus, avec de nombreuses obligations de protection pour les entreprises comme pour les assureurs. Notamment, ces derniers ne doivent plus avoir comme premier réflexe de payer une « petite » rançon en cas d'attaque par rançongiciel, mais de soutenir leur client, quitte à payer plus tard une plus forte perte d'activité liée à cette résistance face à un groupe de cybercriminels.

COURAGE, FUYONS

Début décembre, William Culbert, directeur EMEA Sud de BeyondTrust, éditeur leader de la gestion des accès privilégiés, partageait ses prédictions pour 2022 et anticipait la fin des contrats de cyberassurance.

« Ces dernières années, les polices d'assurance de cybersécurité se sont généralisées dans les entreprises. Malheureusement, les répercussions des attaques de ransomware et d'autres compromissions d'ampleur ont mis à mal le modèle économique des cyberassurances. En conséquence, nombre de cyberassureurs ont augmenté leurs cotisations, cessé d'assurer des entreprises à haut risque ou même quitté le marché des cyberassurances. En 2022, il faut s'attendre à une avalanche d'annulations de cyberassurances et à de grandes difficultés pour se couvrir, avec des cotisations bien plus élevées à la clé. Pour obtenir les meilleures conditions de couverture et de tarifs, les entreprises vont devoir justifier de pratiques de cybersécurité strictes, alignées sur les exigences des assureurs. Et les assureurs n'hésiteront pas à invoquer tout défaut de mise en œuvre des contrôles de cybersécurité préconisés pour refuser l'indemnisation d'un incident ou résilier le contrat » expliquait William Culbert.

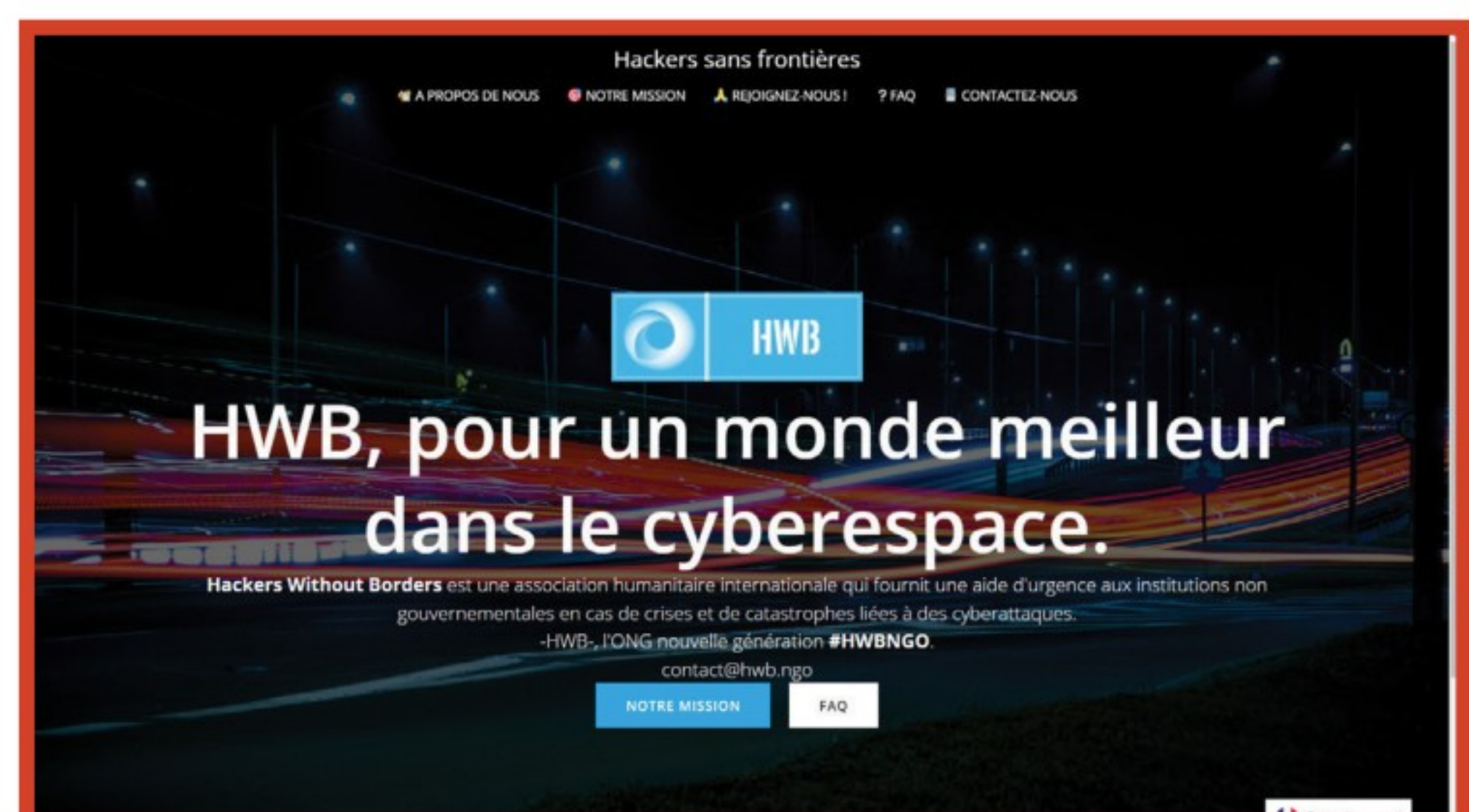


HACKERS SANS FRONTIÈRES

Une nouvelle ONG inédite vient de voir le jour : Hackers sans Frontières. Créée sous l'initiative du Français Karim Lamouri (DSI dans le 93), elle s'est structurée autour d'un ancien gendarme du C3N (unité spécialisée dans la cybercriminalité de la gendarmerie nationale), d'un consultant en cybersécurité et d'un hacker éthique.

Des ONG, internationales ou locales, des hôpitaux ou des centres de ressources pour des populations en difficulté peuvent être, elles aussi, ciblées par des cybercriminels, privés ou institutionnels. C'est le piratage, début 2022, du Comité International de la Croix Rouge (CICR), qui a convaincu Karim Lamouri de monter cette initiative. En réunissant autour d'elle des spécialistes cyber bénévoles, elle veut offrir une cyberprotection, des conseils et des outils aux victimes de conflits armés et d'autres situations de violence. Elle agit en réponse aux urgences tout en promouvant le respect du droit international humanitaire et sa mise en œuvre dans les législations nationales et propose son soutien sans aucun critère de race, de religion, de croyance ou de convictions politiques.

Lien : hwb.ngo/fr



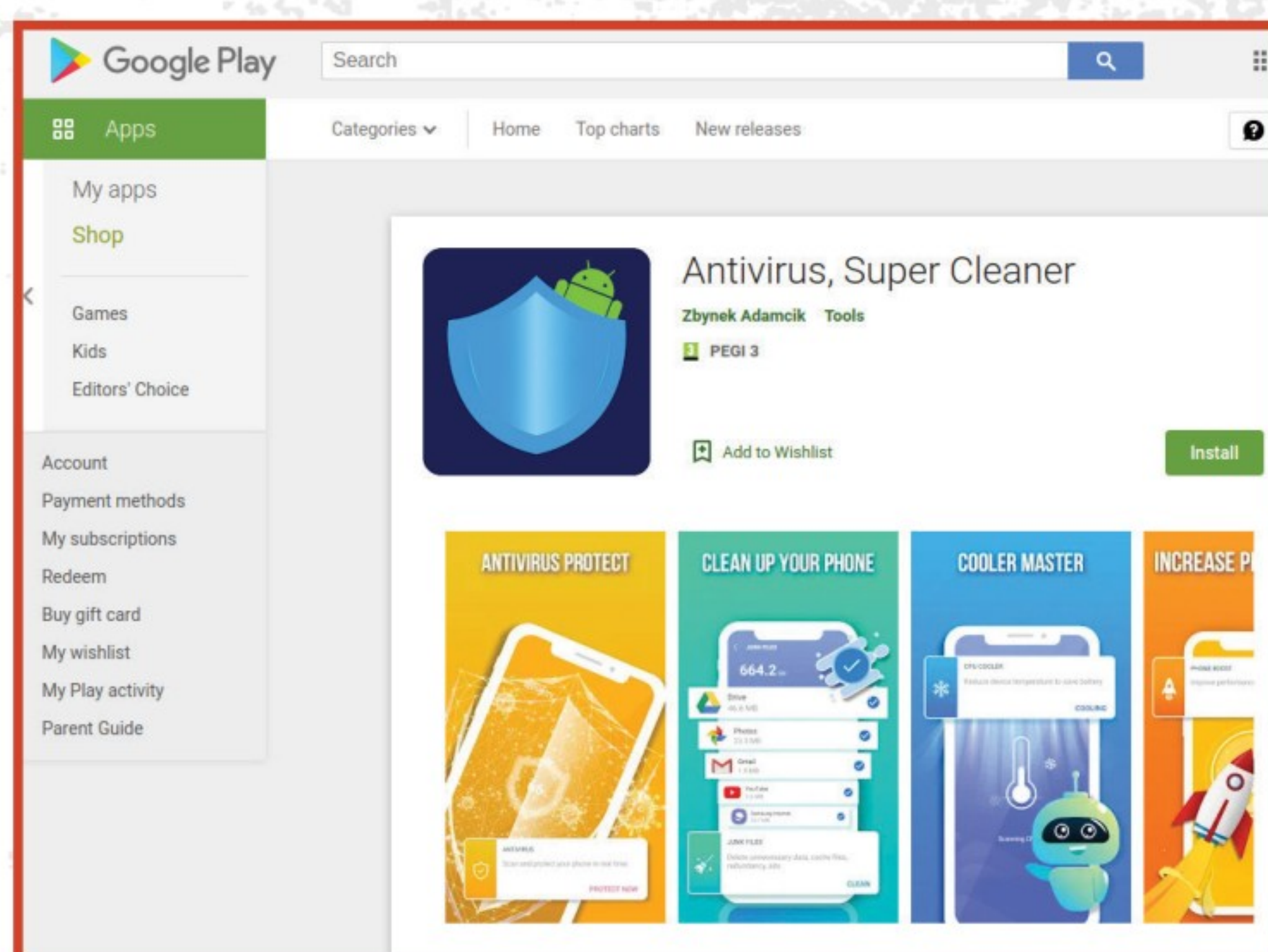
SHARKBOT MENACE VOS COMPTES BANCAIRES

ANDROID

Un nouveau malware s'attaque aux failles de sécurité sur Android. Ce cheval de Troie, baptisé SharkBot, est spécialisé dans le vol de coordonnées bancaires. Ironiquement, pour réussir à s'installer sur le terminal de sa victime... les cybercriminels sont parvenus à l'intégrer à des applis de sécurité et de protection des données !

UN MALWARE HYPER SOPHISTIQUE

Le malware est particulièrement dangereux, car il va se débrouiller tout seul pour repérer les applis bancaires de l'utilisateur et passer des ordres de virement sur d'autres comptes. Pour réussir cet exploit, SharkBot va activer des outils de phishing et de keylogging pour voler les identifiants de la victime. Il pourra même récupérer le code de validation par SMS reçu ! Le malware utilise des systèmes de transfert automatique (ATS) pour demander les virements et il va simuler l'activation des boutons et des touches du clavier pour parvenir à ses fins ! Un programme complet et hyperévolué donc qui fait froid dans le dos...



Toutes les applications vérolées ont été retirées... mais il est évident que SharkBot reviendra dans d'autres applis tant que Google n'aura pas compris comment l'identifier dès son arrivée sur le PlayStore.

VOITURES TESLA PIRATÉES À DISTANCE

Un exploit dont Tesla se serait bien passé. David Colombo, un Allemand de 19 ans, affirme être parvenu à pirater 25 voitures Tesla à distance. Celui qui se présente comme un «spécialiste en sécurité informatique» et un «hacker» ne voulait pas nuire aux propriétaires, mais alerter la firme de Elon Musk sur la faille utilisée. Dans un tweet, il explique être parvenu à ouvrir portes et fenêtres à distance sur des véhicules Tesla... disséminés dans 13 pays européens différents. Il déclare également avoir fait démarrer l'une des Tesla et débrancher son système de sécurité. Il a pu accéder à des informations basiques (présence ou non d'un conducteur, activer la radio, etc.), mais a reconnu qu'il lui était impossible d'initier une conduite à distance.



David Colombo n'a pas communiqué auprès du grand public sur la typologie de cette faille, précisant cependant qu'elle ne concernait pas l'infrastructure Tesla.



MENACES SUR LES VPN

La démocratisation de l'usage des VPN commence à énerver les géants de l'Internet. Au point que certains lancent une chasse discrète, mais résolue contre leurs utilisateurs qui passeraient par ces réseaux virtuels privés. Quitte à faire de nombreuses victimes collatérales.

En février, NordVPN s'alarmait que des membres de Reddit se soient retrouvés « shadow banned » (comprendre non officiellement masqués à la vue des autres utilisateurs), voire définitivement bannis de la plateforme pour usage d'un VPN. Cette corrélation, avérée par les tests des utilisateurs - mais non officiellement reconnue par Reddit - pose encore une fois la question de la neutralité du Net. En effet, en interdisant aux internautes la protection de leur confidentialité en ligne, les plateformes sociales remettent fortement en question la vie privée de ces derniers. Cette pratique de blocage VPN est déjà appliquée par les services de streaming pour des

raisons légales, mais également par des États comme la Chine ou la Russie souhaitant garder la mainmise sur leur trafic.

ENLÈVE TON BOUCLIER POUR ENTRER ICI

Harold Li, vice-président d'ExpressVPN, commente : « Si Reddit interdit effectivement les utilisateurs simplement pour avoir utilisé un VPN, comme certains utilisateurs l'ont signalé, ce serait une mesure décevante et malavisée. »

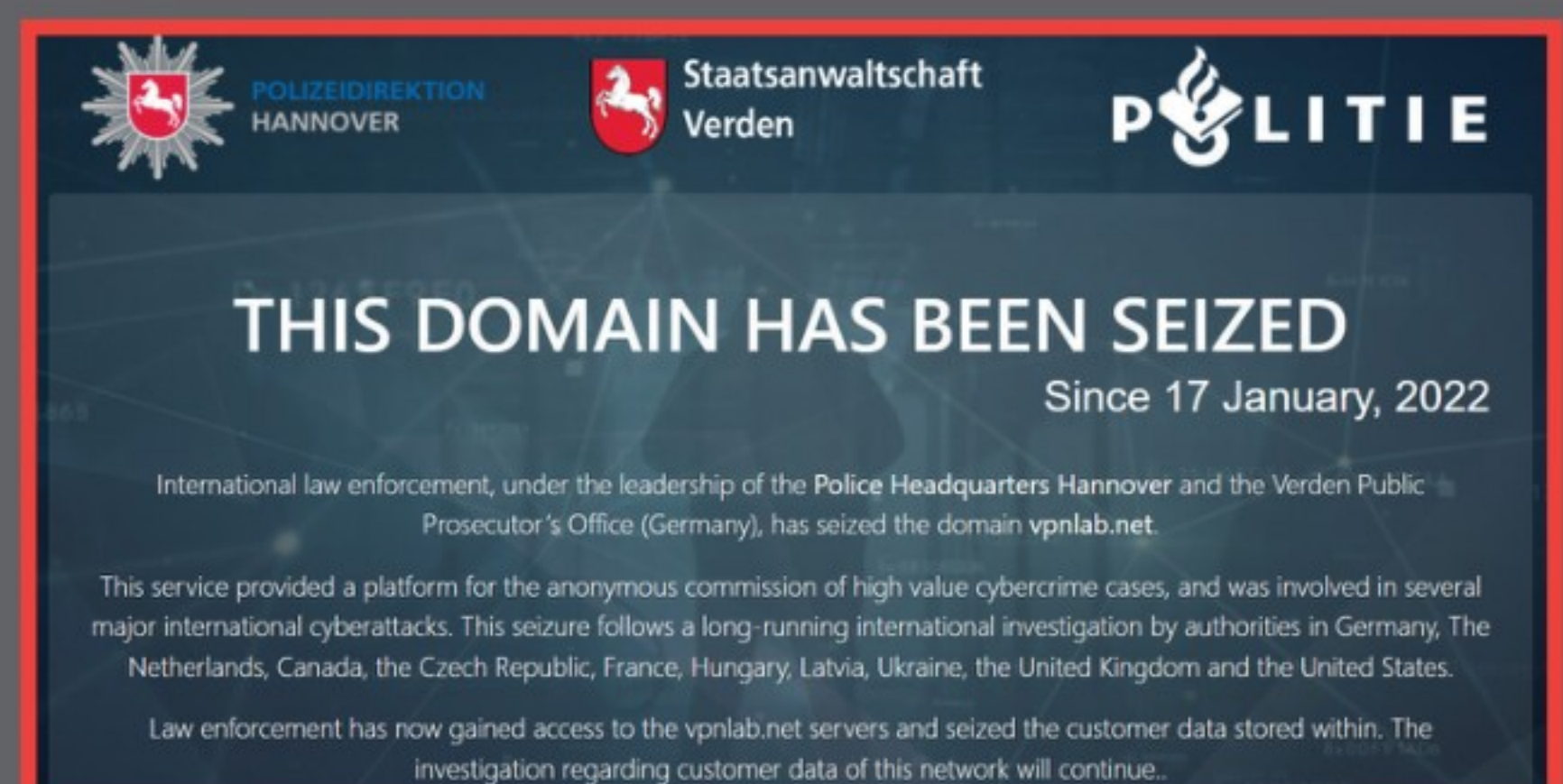
« Lorsque des services bloquent les VPN, ils obligent les utilisateurs à choisir entre l'utilisation du service et la



« SI TOI AVOIR TROP DE CYBERCRIMINELS, MOI FERMER TOI »

C'est un peu la maxime simple à laquelle doit aussi faire attention toute entreprise fournissant un service de VPN.

Une action conjointe d'Europol et des autorités répressives de dix pays (dont la France) a fermé VPNLab en janvier dernier. Ce dernier est accusé d'avoir été utilisé pour commettre des cybercrimes, notamment la distribution de logiciels malveillants et des campagnes de rançongiciels. Le domaine du service affiche désormais une bannière de saisie revendiquant l'implication du service dans des cyberattaques internationales majeures. Personne n'est dupe, un VPN est utilisé pour garantir un certain niveau d'anonymat et de confidentialité. On peut imaginer que tous les VPN abritent une part d'utilisateurs « ayant quelque chose à cacher », y compris une activité illégale. Alors pourquoi avoir ciblé spécifiquement VPNLab ?



FAIRE DE LA PUB SUR LE DARKNET : MAUVAISE IDÉE

Pour rester dans les limites de la loi, le facteur important est de savoir si le fournisseur ou le service de communication encourage ou facilite activement et sciemment des activités

protection de leur vie privée et de leur sécurité », poursuit-il. « Ce n'est pas un choix que quiconque devrait avoir à faire, en particulier les utilisateurs vulnérables, et notamment sur les plateformes d'expression, d'échange d'informations et d'association. »

NETFLIX BLOQUE SES PROPRES CLIENTS!

Du côté de Netflix, la « guerre contre les VPN » est plus ancienne. L'entreprise américaine scanne en permanence les adresses IP qui seraient attribuées à tel ou tel serveur venant d'un VPN. Ces derniers jouent au chat et à la souris en renouvelant incessamment ses paquets d'adresses IP afin que leurs utilisateurs ne soient pas bloqués. Mais, ces derniers mois, ce « jeu » fait des victimes collatérales ! Pour contourner le geoblocking de Netflix, les VPN acquièrent des plages d'IP résidentielles (c'est-à-dire attribuées à la distribution de lignes fixes dans telle ou telle région précise). Pour Netflix, rien ne ressemble plus à un vrai client que ce type d'IP ! Seulement, la plateforme a fini par se rendre compte du stratagème. Et elle bloque de plus en plus ce type de plages. Malheureusement, beaucoup de clients physiques et qui paient leurs abonnements sont aussi reliés à ces plages d'IP résidentielles ! Du coup, hop, dans le même sac : service bloqué ou limité par Netflix. Selon WeVPN, interviewé sur TorrentFreak, « Des centaines de milliers d'abonnés résidentiels légitimes de Netflix sont bloqués pour accéder au catalogue complet de leur région depuis leur domicile ».



UN OUTIL PUISSANT ADOPTÉ PAR LE GRAND PUBLIC

Depuis cinq ans, les VPN ont conquis le grand public. Pour un tarif mensuel raisonnable (quelques euros), ils offrent trois avantages majeurs :

- Chiffrer et tunneliser les données des utilisateurs afin de les protéger des regards extérieurs. Un gage de sécurité et de protection de la vie privée indéniable ;
- Masquer la localisation de leur requête ;
- Pouvoir au contraire choisir une localisation étrangère, permettant d'accéder à tel ou tel service normalement indisponible ou limité dans le pays de l'utilisateur.

Et nous n'allons pas nous mentir, qu'il s'agisse d'accéder à des sites de streaming et de téléchargements illégaux ou à la plateforme américain de Netflix (beaucoup plus de contenus!), ce dernier avantage explique en partie le succès des VPN en Europe, et plus particulièrement en France.

illégal. Europol s'est intéressé à VPNLab parce que ce dernier a eu la mauvaise idée de faire sa promotion sur le Darknet, sur des forums et des sites oignons abritant de nombreuses activités illégales. Sous l'apparence d'un VPN tout à fait classique, il semble que VPNLab draguait ouvertement ce type de clientèle au point de représenter une menace systémique bien identifiée.

L'action contre VPNLab fait suite à une opération similaire menée en juin 2021 contre DoubleVPN. Dans cette affaire, le fournisseur de VPN a également été accusé d'être complice des actions de ses utilisateurs, non seulement en fournissant l'anonymat, mais en se faisant de la publicité sur les forums de cybercriminalité comme un moyen pour les opérateurs de rançongiciels et les fraudeurs de phishing de cacher leurs emplacements.

RISQUE D'ABUS DE POUVOIR

Une question demeure : à partir de quel taux de cybercriminels décide-t-on de fermer tel ou tel service de VPN ? Tout est à la discrétion des autorités, seules à même de mesurer la menace. Ce qui est inquiétant, c'est la pression qui peut ainsi être mise sur les sociétés VPN : de plus en plus d'États exigent que ces dernières conservent un minimum de données sur leurs utilisateurs (logs) ou disposent même d'une backdoor en cas d'enquête. Alors que les VPN sont censés justement éviter ce type de risques et de dérives ! « Un aspect important de cette action (Ndlr : contre VPNLab) est également de montrer que, si les fournisseurs de services soutiennent les actions illégales et ne fournissent aucune information sur les demandes légales des autorités chargées de l'application des lois, ces services ne sont pas à l'épreuve des balles », a déclaré Volker Kluwe, chef du département de police de Hanovre et partie prenante de l'enquête Europol. Une menace à peine voilée...

MALWARES

GOOGLE CLOUD S'ARME CONTRE LE CRYPTOMINING

Fin 2021, la Cybersecurity Team de Google estimait que 86 % des attaques réussies sur les services de cloud visaient à effectuer du minage de cryptomonnaies via les comptes des clients piratés. Google Cloud a développé et intégré un nouvel outil anti-cryptomining, sa Virtual Machine Threat Detection (VMTD), disponible via le Security Command Center (SCC) de Google.

VMTD analyse les instances Compute Engine dans Google Cloud pour détecter les menaces telles que les logiciels malveillants de cryptomining utilisés dans les machines virtuelles. VMTD collecte les signaux sans exécuter de logiciel supplémentaire – permettant ainsi de diminuer les surfaces d'attaque exposées, sans pour autant, amoindrir les performances.

Outre la lutte contre le minage de cryptomonnaies, VMTD permet aussi de contrer l'exfiltration de données et les ransomwares.



QUANTIQUE VS BLOCKCHAIN

COMBIEN DE QUBITS POUR PIRATER UN BITCOIN?

En théorie, il est impossible de compromettre et de pirater la blockchain, ce système informatique complexe et récent qui sécurise notamment la création, la distribution et la valorisation des cryptomonnaies. En tout cas, les ordinateurs les plus puissants du monde, même les ordinateurs quantiques en développement, seraient bien incapables de fournir des algorithmes et des puissances de calcul suffisants. Mais comme jamais rien n'est définitivement impossible, Max Webber, de la start-up Universal Quantum, s'est amusé à estimer le nombre de qubits (unité mesurant la puissance de calcul en informatique quantique) pour pénétrer cette forteresse blockchain.

317 MILLIONS (OUI, C'EST LA RÉPONSE)

« Lorsque quelqu'un effectue une transaction en bitcoin, celle-ci est annoncée au monde entier, mais elle n'est pas totalement sécurisée tant qu'elle n'a pas été intégrée à la blockchain », souligne Mark Webber. C'est dans ce laps de temps (variable, de 10 min à 1 journée) qu'une attaque pourrait être lancée. Mais il faudrait une puissance de feu phénoménale. Si l'on disposait par exemple d'une heure, l'équipe de Mark Weber a estimé qu'il faudrait environ 317 millions de qubits pour pirater un bitcoin. Pour rappel,



les ordinateurs quantiques les plus puissants actuels atteignent entre 100 et 150 qubits seulement. La blockchain retient un sourire poli... Mark Webber prévient cependant : il a montré qu'un piratage n'est pas impossible et qu'une faille existe. Et rien ne dit que l'évolution des puissances de calcul quantique ne sera pas exponentielle comme ce fut le cas pour l'informatique classique.

ENQUÊTE

LES FRANÇAIS ET LES CRYPTOS : « ÇA M'INTÉRESSE, MAIS J'AIME PAS TROP »

Afin de mesurer la connaissance et l'intérêt des Français pour ces actifs numériques, le média spécialisé **Cointribune.com** a confié à l'Ifop le soin d'interroger plus de 2 000 personnes.

L'étude de février 2022 montre notamment que si nos compatriotes ont massivement entendu parler des cryptomonnaies, Bitcoin en tête, les NFT restent l'apanage d'un public jeune et initié. Globalement, les Français restent sceptiques sur ces produits qu'ils considèrent davantage comme un phénomène de mode spéculatif à la rentabilité incertaine que comme des investissements crédibles sur le moyen et long terme. Mais cette photographie générale ne doit pas masquer l'attrait grandissant de la jeune génération, les 18-24 se distinguant clairement de leurs aînés dans leur volonté d'investir dans le monde numérique. La connaissance des actifs numériques est plutôt l'apanage d'hommes jeunes, diplômés de l'enseignement supérieur, appartenant aux classes aisées et résidant dans l'agglomération parisienne.

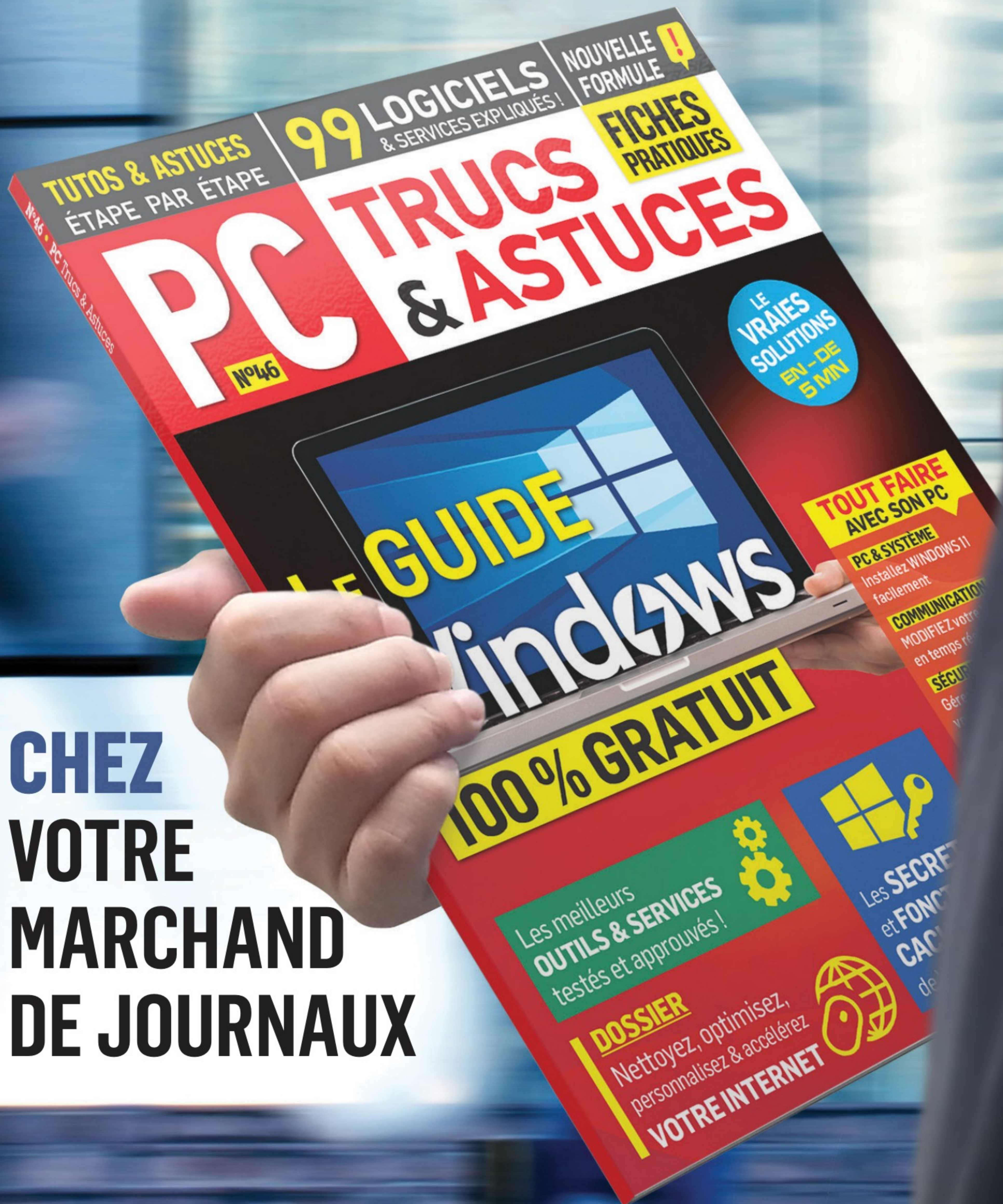
SI HUIT FRANÇAIS SUR DIX CONNAISSENT LES CRYPTOS, ILS NE SONT QUE 5 % À AVOIR DÉJÀ ACHETÉ UN BIEN PHYSIQUE AVEC. L'ENQUÊTE IFOP, PUBLIÉE SUR COINTRIBUNE, CONFIRME UN FOSSÉ GÉNÉRATIONNEL, NOTAMMENT POUR LES ACTIFS NFT - QUASI INCONNUS CHEZ NOS ÂÎNÉS.

LES CHIFFRES CLÉS DE L'ENQUÊTE :

- **82%** des Français ont entendu parler des cryptomonnaies alors qu'ils n'étaient que 52% en février 2021 ;
- Les NFT ne sont arrivés aux oreilles que d'1 Français sur 4 (**25%**) et seulement **8%** savent précisément de quoi il s'agit ;
- **40%** des 18-34 ans qui connaissent les cryptomonnaies ont investi dans ces actifs numériques ou seraient prêts à le faire contre **18%** des plus de 35 ans ;
- Seuls **5%** déclarent avoir acheté un objet avec de la cryptomonnaie sur une plateforme compatible... et **2%** aussi à avouer avoir déjà acheté quelque chose d'illégal avec (drogue, marché noir, ...) ;
- **22%** des Français se déclarent cependant prêts à régler des achats en ligne et **15%** à être payés en Bitcoin ;
- Près de la moitié (**49%**) des jeunes de 18 à 24 ans pourraient acheter un objet numérique sous forme de NFT contre seulement **8%** des plus de 65 ans ;
- Chez les connaisseurs des cryptomonnaies, ils sont **41%** à voir la valeur du marché augmenter et **16%** à penser qu'elle baissera ;



L'INFORMATIQUE FACILE POUR TOUS !



**CHEZ
VOTRE
MARCHAND
DE JOURNAUX**

RÉSISTER À L'OGRE RUSSE



LES LEÇONS D'UNE CYBERGUERRE

Les quinze premiers jours de conflit entre la Russie et l'Ukraine ont été riches en surprises côté cyberspace. La géopolitique cyber s'en trouve même bouleversée et de nouveaux rapports de force sont apparus.

À l'aube du jeudi 24 février, premier jour de l'offensive russe en Ukraine, la question d'une cyberguerre menée par la Russie, en parallèle de la guerre classique, inquiétait déjà nombre d'observateurs. C'est que l'ogre russe fait peur dans le cyberspace. Il serait techniquement très pointu, sans foi ni loi, sa puissance de feu réelle est méconnue et il disposerait de bataillons entiers prêts à répandre la cyber-désolation au-delà des frontières russes. Les attaques ne viseraient-elles que l'Ukraine, l'Europe devait-elle s'inquiéter ? Quinze jours après le début du conflit, c'est la surprise. Certes, les cyberattaques sont quotidiennes en Ukraine, de nouvelles armes ont été utilisées... mais le pays tient bon et on commence à s'interroger sur les réelles capacités de la Russie. À l'image du conflit « classique » finalement.

LE CYBERESPACE UKRAINIEN N'EST PAS TOMBÉ

Ralentissements, pannes temporaires, sites Web inaccessibles quelques heures : les perturbations sont réelles, quotidiennes, mais réseau et infrastructures tiennent bon, sauf dans les zones où des centres

de communication ont été détruits ou sabotés physiquement par l'armée russe. L'équipe de recherche Internet de ThousandEyes a noté la disponibilité réduite des sites Web ukrainiens clés dans le domaine bancaire, de la défense et d'autres sites gouvernementaux.

Le blitzkrieg
numérique
n'a pas eu lieu



« Les perturbations reflètent bien le comportement du réseau que nous avons observé dans d'autres attaques par déni de service distribué (DDoS), et témoignent des contre-mesures potentielles qui ont pu être prises par les opérateurs de service pour atténuer les impacts sur leur activité », a déclaré ThousandEyes le 4 mars. Notamment, la parade ukrainienne pour sécuriser ses services de cloud pour déporter les attaques DDos s'est avérée efficace. « Les entreprises ukrainiennes semblent prendre des mesures défensives en bloquant le trafic sélectif provenant de Russie et, dans certains cas, de Chine », a encore déclaré ThousandEyes.

PAS DE COUPURE CENTRALE

Quant à Internet, là aussi les attaques sont constantes et le réseau disparaît dans tel ou tel endroit avant de réapparaître avec une surprenante résilience. « *L'Ukraine dispose d'une infrastructure Internet diversifiée avec peu de points d'étranglement, ce qui signifie qu'il est difficile de mettre le pays hors tension, et qu'il n'y a pas de coupe-circuit centralisé* », a déclaré Alp Toker, fondateur et directeur de NetBlocks, au Guardian. « *Si un envahisseur voulait couper l'Internet ukrainien, il faudrait qu'il pénètre physiquement dans les points d'interconnexions Internet (IXP) et les datacenters et qu'il prenne le contrôle de cette infrastructure.* »

DE NOUVELLES ARMES TESTÉES

« *Plusieurs heures avant le lancement des missiles ou le déplacement des chars le 24 février, le MSTIC a détecté une série de cyberattaques offensives et destructrices contre l'infrastructure IT de l'Ukraine* », a déclaré Brad Smith, président de Microsoft. Et d'ajouter : « *Nous avons immédiatement informé le gouvernement ukrainien de la situation, notamment de l'identification d'un nouveau malware (que nous avons dénommé FoxBlade) et nous avons fourni des conseils techniques sur les mesures à prendre pour empêcher cette menace* ». FoxBlade est un nouveau cheval de Troie destiné à multiplier la puissance de feu des attaques DDos (survenues elles dès le début de la guerre). Son efficacité a été heureusement limitée grâce à la coopération technologique immédiate entre les États-Unis et l'Ukraine.

LA RUSSIE ENVOIE SES NETTOYEURS

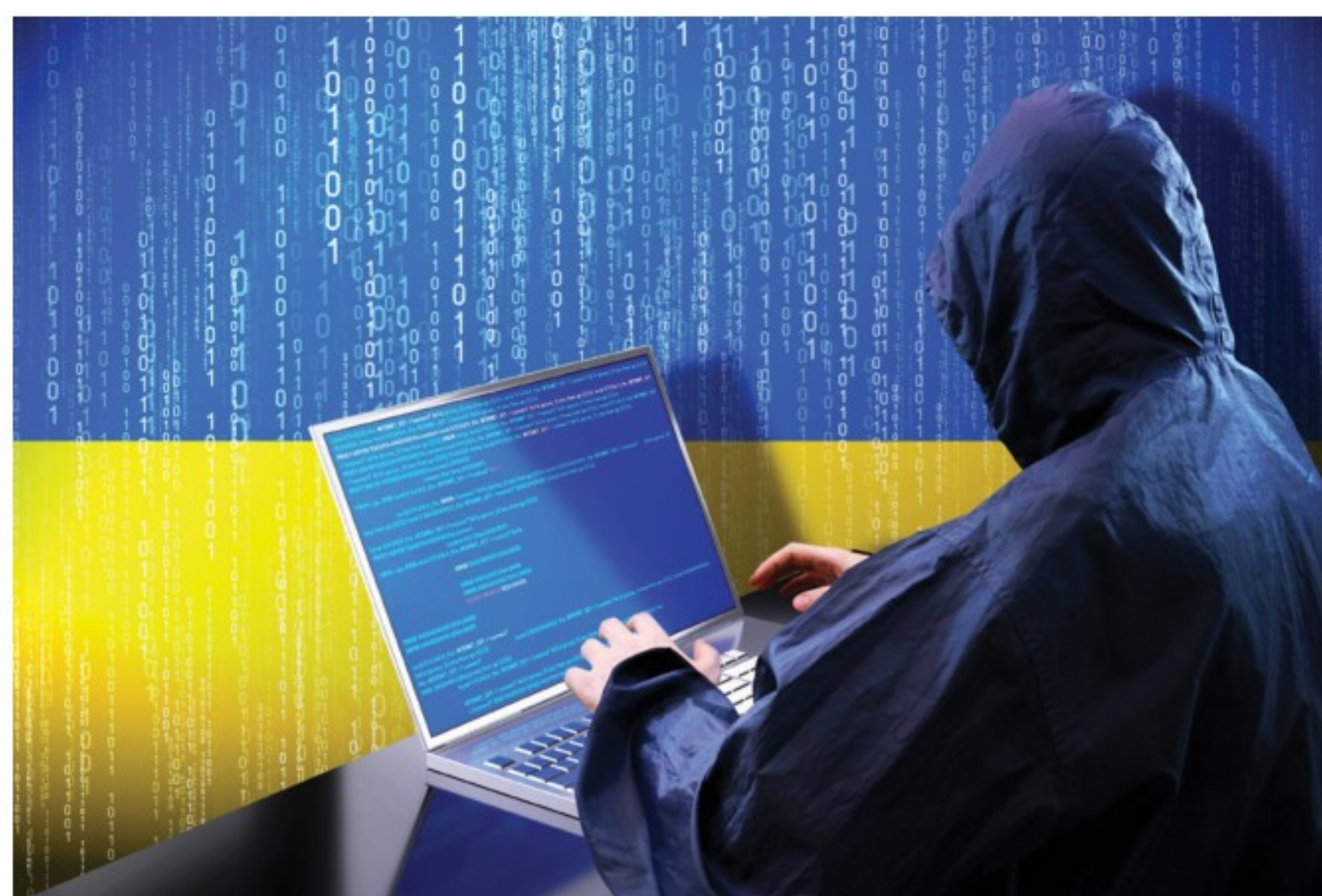
Le malware dont on a le plus entendu parler est HermeticWiper, un « effaceur » de données particulièrement puissant et discret qui a visé des institutions et des centres de communication. Ici, pas de vol de données ou de blocage : si le malware s'active sur une unité de stockage, il va tout simplement tout effacer de façon rapide et, semble-t-il, définitive. Un phénomène similaire avait été observé avec la souche WhisperGate masquée en payload de ransomware. Cet agent fait peur, mais, alors qu'il masquait sa signature par un certificat valide et sous couvert d'autres malwares moins puissants, il serait aujourd'hui identifié par les solutions de sécurité.



LES « EFFACEURS » (WIPERS EN ANGLAIS) SONT DES MALWARES QUI N'ONT QU'UN OBJECTIF : SUPPRIMER TOUTES LES DONNÉES D'UNE UNITÉ DE STOCKAGE QU'ELLES AURAIENT INFECTÉ.

DES CONTRE-ATTAQUES INTERNATIONALES

La Russie ne s'attendait pas à ce retour de flamme. Dès les premiers jours de son offensive, comme sur le terrain, de nombreuses entreprises et institutions russes ont subi les sanctions du cyberspace mondial. L'indignation suscitée par



L'ESPACE, NOUVELLE EXTENSION DU CONFLIT

Les satellites sont aussi devenus des enjeux cruciaux pour la conduite des opérations au sol. Le National Reconnaissance Office (NRO), bureau fédéral des renseignements aux États-Unis, a lancé les premières alertes, pointant la cyberattaque du satellite de télécommunication KA-SAT de la compagnie américaine Viasat. Ce satellite desservait l'Europe et notamment l'Ukraine. Le 4 mars, la compagnie américaine HawkEye 360, spécialisée dans l'analyse géospatiale, repérait également des interférences dans les communications radio entre le sol et le réseau GPS d'Ukraine. Grâce à la collaboration internationale, les autorités ukrainiennes ont pu accéder à d'autres sources pour garantir une maîtrise suffisante de leur surveillance depuis l'espace.

cette agression a mobilisé des hackers individuels ou des collectifs (comme les Anonymous) qui ont lancé des attaques permanentes au cœur du plus grand pays du monde.

70 % DES ATTAQUES.. CONTRE LA RUSSIE!

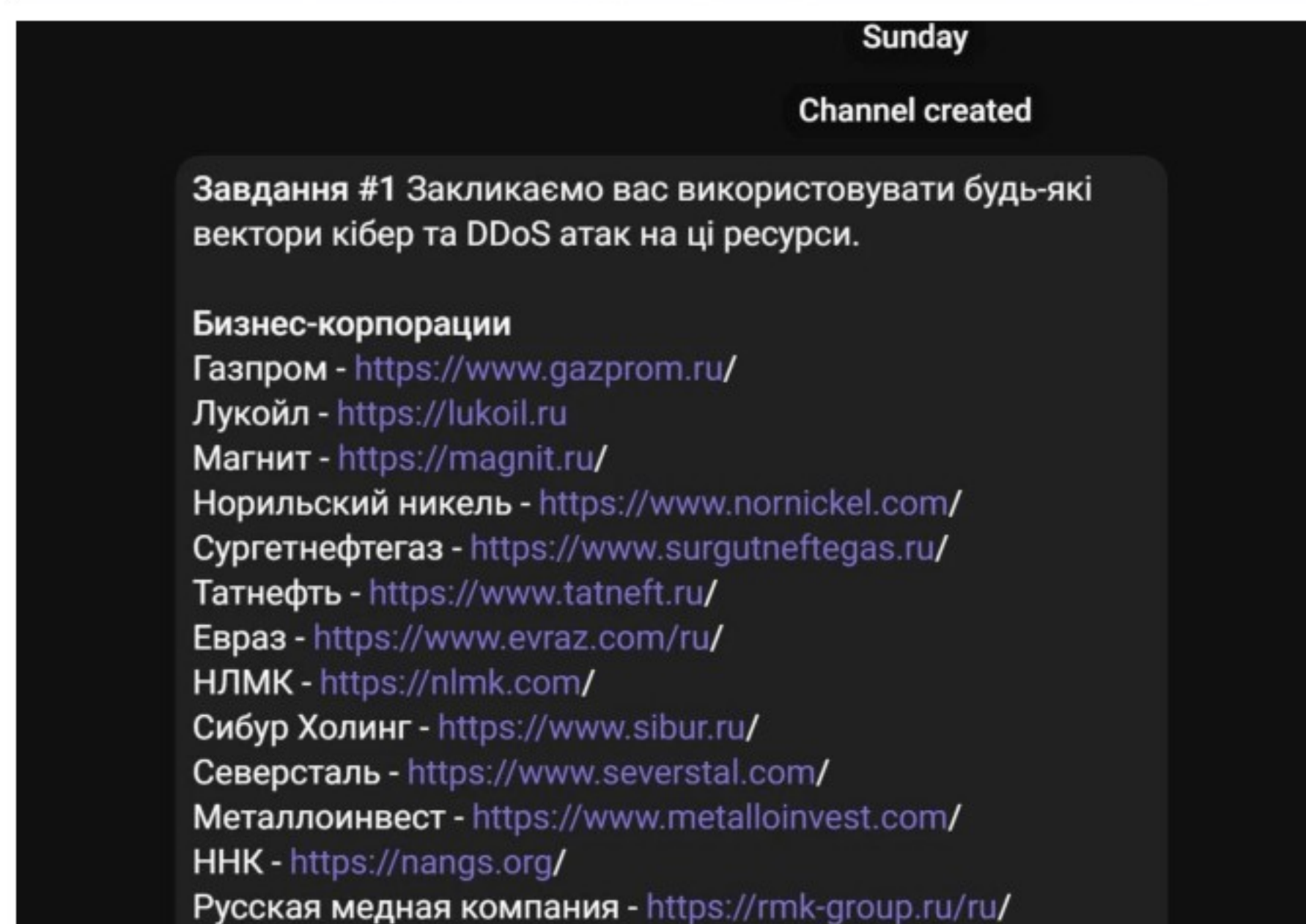
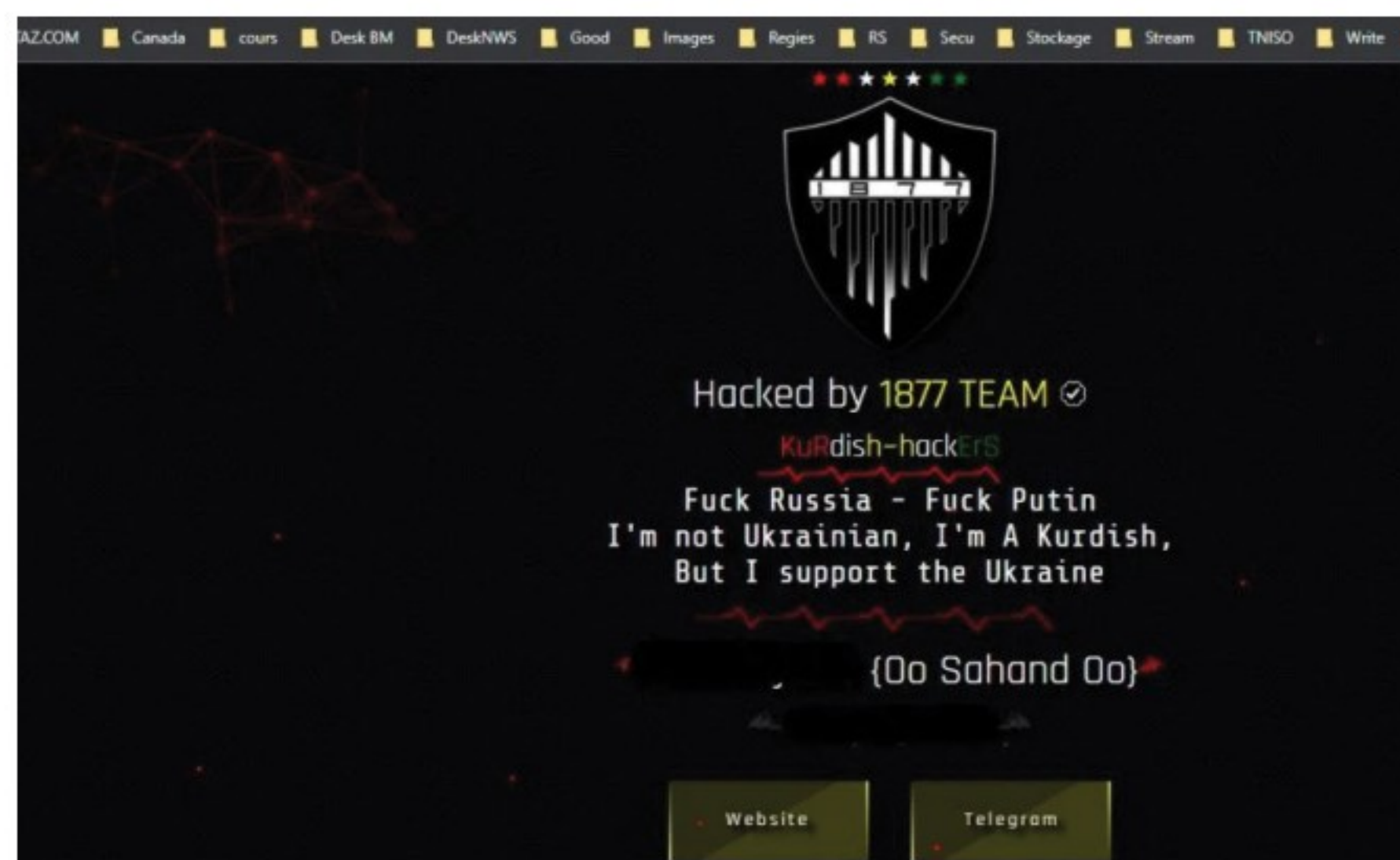
Ainsi, l'agresseur se retrouve l'agressé : début mars, selon AtlasVPN, cinq milliards d'attaques ont été dirigées vers le pays, soit 70 % des cyberattaques mondiales alors que « seulement » 19% ont visaient l'Ukraine et 5 % les États-Unis. Un renversement intéressant qui oblige notamment les forces de cybersécurité russes à consacrer énormément de temps à la défense... et beaucoup moins à l'attaque, ce que personne ne regrette.

Comme l'Ukraine a fait appel à des volontaires du monde entier pour venir se battre à ses côtés, elle a aussi lancé un appel à tous les hackers (pros ou du dimanche) qui souhaitaient rejoindre sa cyberarmée. Le ministre en charge de la transformation digitale, Mykhailo Fedorov, a lancé un appel aux armes numériques « Nous créons une armée informatique. Nous avons besoin de talents numériques. [...] Il y aura des tâches pour tout le monde. Nous continuons à nous battre sur le front cybernétique. »

BRIGADES CYBER INTERNATIONALES

Damien Bancal, éditeur du site Zataz.com, a voulu voir de l'intérieur en quoi consistait cette « IT Army of Ukraine » en rejoignant la chaîne Telegram dédiée. Une liste de sites institutionnels et privés russes est par exemple fournie et on invite les membres à lancer contre elles des attaques DDos. ZATAZ a également pu référencer une centaine de sites russes défacés, barbouillés par des « indépendants ».

Selon Damien Bancal, le type de cible change en permanence, on passe d'influenceurs à signaler au blocage de banques, de sites marchands ou... de distributeurs de billets. Le journaliste spécialisé avoue sa gêne et ses interrogations : qui décide ? Les membres mesurent-ils l'illégalité de nombreuses actions qu'ils entreprennent ou accompagnent ? N'y a-t-il pas le risque de nombreux dérapages au sein de cette cyberarmée anarchique ?



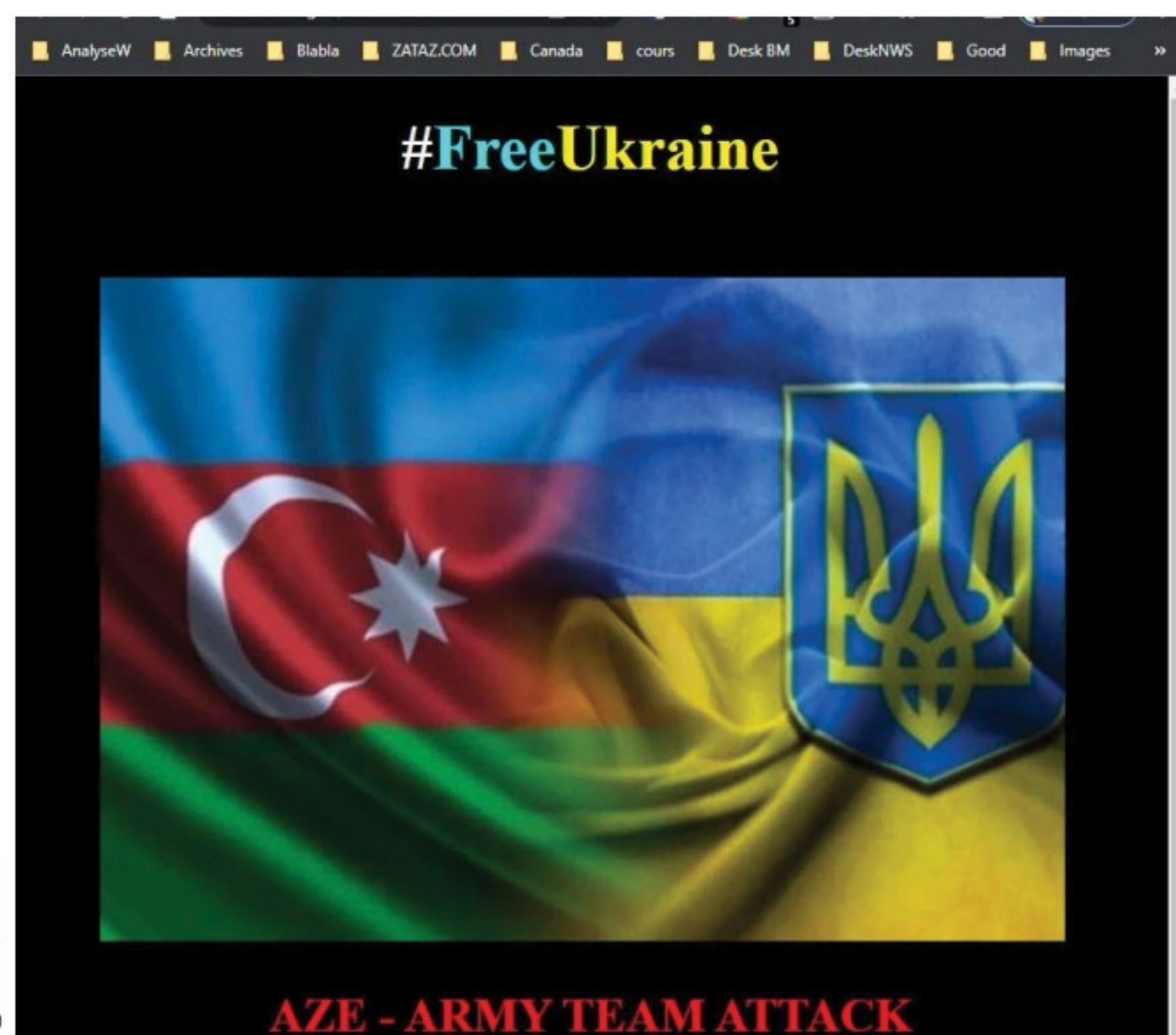
LA MENACE DE L'OTAN

Dès le début de la guerre, les Occidentaux ont fait savoir à leurs homologues russes que toute action cyber d'importance menée contre l'un des membres de l'OTAN serait considérée comme une agression qui entraînerait une riposte mutuelle. Est-ce que cela a effectivement freiné les ardeurs du Kremlin ou est-ce que le niveau d'alerte cyber rehaussé aux USA et en Europe a suffi à déjouer les principales attaques ? En tous cas, à l'heure où nous écrivons ces lignes, l'ogre russe n'a pas sorti ses griffes. Enfin, pas plus que d'habitude.



COMCYBER : LA DISSUASION FRANÇAISE

Notons que la France a fait évoluer sa doctrine cyber ces dernières années. D'une approche purement défensive, elle opte désormais pour une politique hybride : je n'attaque pas en premier, mais si tu m'attaques, je me défends puis je contre-attaque. Pour mettre en pratique cette menace, c'est le ComCyber de Rennes qui sert de vaisseau amiral. Ce centre, qui doit employer à terme plus de 5000 personnes, est le nouveau centre de projection cyber de nos soldats numériques. Il a l'autorisation de mener des offensives proportionnées et ne visant pas les civils contre un agresseur cyber, qu'il soit mafieux, institutionnel... ou étatique.



APPLIS EN TEMPS DE GUERRE

Voici quelques exemples d'applications qui ont vu leurs téléchargements s'envoler en Ukraine sur GooglePlay au cours des 15 premiers jours de guerre, jusqu'à atteindre le TOP 10, même temporairement.



Signal > Pour les échanges sécurisés bien sûr.



Дія (Diya) > Une application du ministère ukrainien de la transformation digitale. Elle permet aux citoyens ukrainiens de retrouver leurs papiers officiels (carte d'identité, passeport ...) de façon numérisée et valide. Indispensable pour les check-points ou quand on s'apprête à fuir le pays.



Повітряна тривога (Air Alarm) > Pour recevoir instantanément une notification d'alerte aérienne dans la ville ou la région d'Ukraine de votre choix à partir du système de défense civile.



Bridgefy > Bridgefy vous permet d'envoyer des messages hors ligne à vos amis et à votre famille à moins de 100 m lorsque vous n'avez pas accès à Internet, en activant votre Bluetooth et un réseau de type mesh.



Offline-Games-No-Wifi > Un bundle de centaines de petits jeux accessibles sans Internet. Parce que passer des nuits entières dans le métro, voilà quoi...



Zello Walkie Talkie > Une application qui permet de capter les ondes radio. Pour information, de nombreux soldats russes utilisaient des talkies-walkies non sécurisés et ont pu être écoutés par la population et les militaires ukrainiens !



Maps.me > Utilisé par les civils, mais aussi par les soldats des deux parties ! Utile pour repérer un embouteillage de tanks... Surtout, son système de navigation offline est la vraie raison de son succès.



Briar > Une application de messagerie conçue pour les militants et les journalistes pour communiquer plus discrètement. Sans serveur central, les messages sont synchronisés directement entre appareils. Si Internet est en panne, Briar peut se synchroniser via Bluetooth ou Wi-Fi. Si Internet fonctionne, Briar peut se synchroniser via le réseau Tor.



MaxSpeedfry-Unlimited&Easy > Un proxy gratuit pour se connecter depuis un autre pays. Réputé pour sa stabilité et sa rapidité.



APPLIS DE RENCONTRES LES SERVICES SECRETS UKRAINIENS VOUS REMERCIENT!

Les soldats russes sont vraiment venus en Ukraine la fleur au fusil. Persuadés sans doute d'arriver en libérateurs acclamés par des foules en liesse, pourquoi ne pas en profiter pour faire quelques rencontres ? Les applis Tinder et Grindr ont permis aux services de renseignements occidentaux et ukrainiens de repérer la position de certains soldats qui cherchaient à matcher avec des Ukrainiens et des Ukrainiennes.

Beaucoup se montraient armés, donnaient quelques indications sur leur programme de visite à venir... Le MI6, le service de renseignements britannique, a alerté et transmis en ce sens de nombreuses informations à son homologue ukrainien, l'aidant à repérer notamment leurs positions exactes grâce à la géolocalisation. Dès que l'info a fuité, l'utilisation de ces applis a été interdite côté russe.

CRYPTOMONNAIES : UNE VALEUR REFUGE?

Pour les Russes, les cryptomonnaies peuvent-elles être une solution pour échapper aux sanctions financières ?

Les principales sanctions européennes visaient à étrangler les capacités de financement de l'état et du secteur privé, tout en gelant les avoirs internationaux de nombreux oligarques. Dégringolade du rouble, moyens de paiement en berne (Swift, Visa, Mastercard, American Express), déconnexion partielle de la finance mondiale,

personnes visées par les sanctions internationales si elles étaient identifiables. À elle seule, Coinbase aurait identifié 25000 comptes (!) ayant « *un lien direct ou indirect avec des personnes et entités qui posent problème* », a expliqué le responsable juridique du groupe, Paul Grewal.



difficultés d'accès aux devises étrangères, etc. : les Russes ont dû trouver des solutions alternatives. L'or comme d'habitude a servi de première valeur refuge pour la banque centrale russe, comme pour les particuliers. Et puis tout le monde s'est bien sûr posé la question des cryptomonnaies. Et si on achetait des brouettes entières de bitcoins ??

DES VOLUMES D'ÉCHANGE EN HAUSSE

À l'annonce du début de la guerre, le cours s'est effondré, comme tous les autres actifs financiers. Avant de remonter en flèche. La crypto est remontée à 43600 dollars le 1er mars et les échanges de cryptos en roubles triplaient depuis début février (60 millions de dollars par jour selon Chainalysis, cité par le *Financial Times*). Et plus que le Bitcoin, c'est le Tether, une « stablecoin » jugée moins volatile qui était plébiscitée. La ruée vers le Bitcoin était en cours.

Dès fin février, le vice-premier ministre ukrainien, Mykhailo Fedorov, demandait aux principales plateformes d'échange de cryptos de bloquer les comptes des résidents russes. Ces dernières n'ont pas donné suite à cette demande générale, mais ont bel et bien commencé à cibler les avoirs des

L'EFFONDREMENT DU ROUBLE ET LES BLOCAGES FINANCIERS ONT POUSSE DES MILLIERS DE RUSSES À INVESTIR DANS LES CRYPTOMONNAIES. MAIS LES PLATEFORMES D'ÉCHANGE ET DE TRADING SPÉCIALISÉES SE SONT AUSSI MISES À GELER LES AVOIRS DES PERSONNES ET ENTITÉS SANCTIONNÉS PAR L'OCCIDENT.



L'ÉTAT RUSSE HÉSITE

Côté Kremlin, et depuis la fin d'année dernière, la volonté affichée était paradoxalement d'interdire le minage et la circulation de cryptos. Enfin, pas pour tout le monde. Ivan Chebeskov, directeur de la politique financière au sein du ministère des Finances en Russie, a arrondi les angles en janvier : « *Nous devons donner à ces technologies la possibilité de se développer. À cet égard, le ministère des Finances participe activement à l'élaboration d'initiatives législatives en termes de réglementation de ce marché* ». En février, l'idée était bien de réglementer... et même de définir « le cercle des participants autorisés ». Soviet un jour, soviet toujours.

ARMÉE INTERNET d'UKRAINE

200000 FANTASSINS À LA CONQUÊTE DU MONDE

« À cause de la propagande, les Russes ne savent pas ce qu'il se passe vraiment en Ukraine. (...) Notre but est de corriger ça », explique l'un des administrateurs de la chaîne Telegram Інтернет Війська України (Armée Internet d'Ukraine).

Plus qu'un bataillon, c'est une véritable armée : forte de 200000 membres, principalement ukrainiens, l'Armée Internet d'Ukraine s'est lancée dans la guerre de l'information via Telegram.

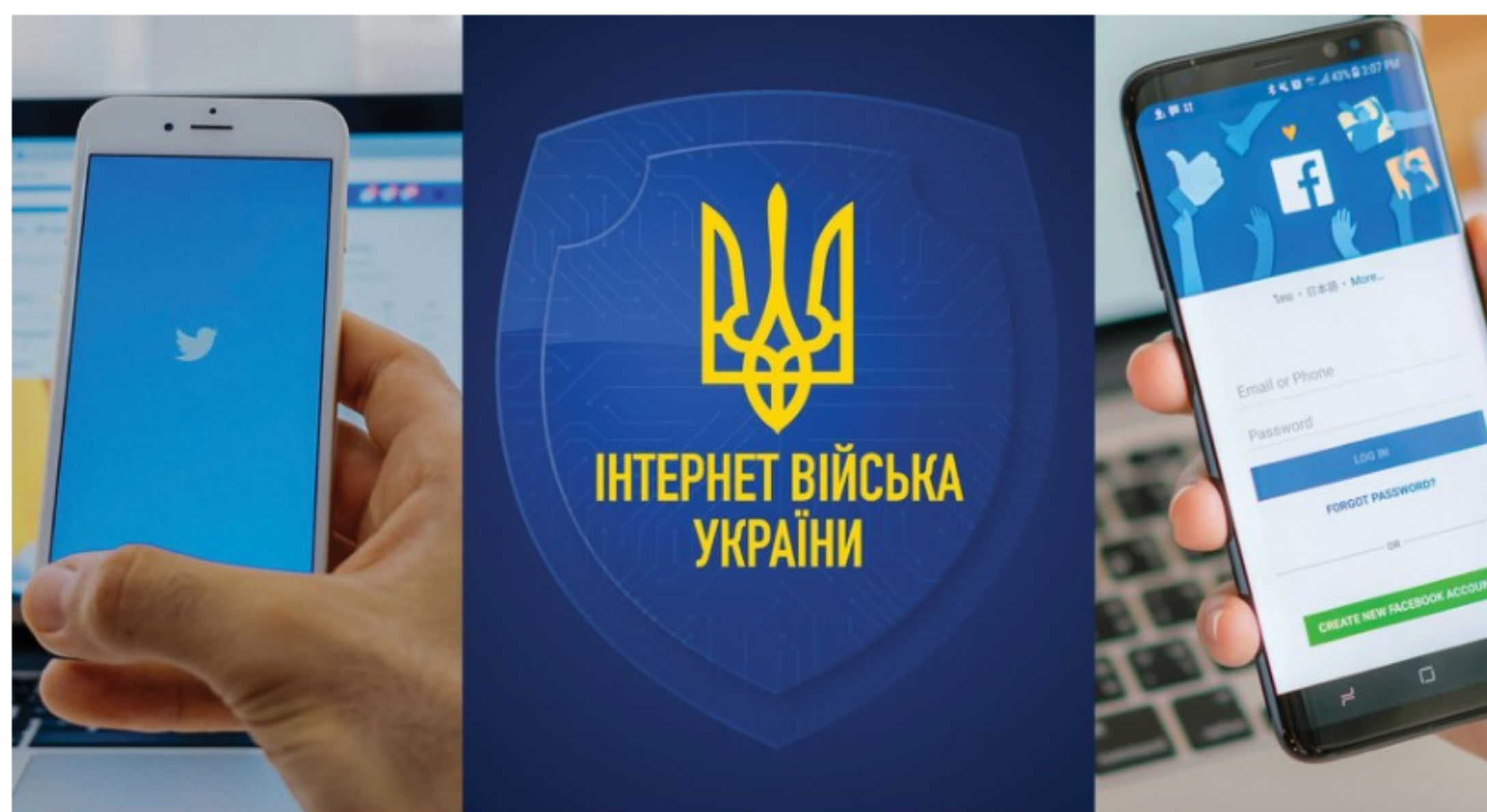
EN ORDRE DE MARCHÉ

Et la division du travail est bien orchestrée, notamment en collaborant avec d'autres chaînes Telegram spécialisées dans la « production ». Montage vidéo ou photos, textes, mêmes, cibles à atteindre, stratégies marketing, etc. : chacun, à la mesure de ce qu'il sait et peut faire, offre ses compétences. L'objectif est double :

- 1) Sensibiliser les gouvernements, grandes entreprises et opinions publiques à ce qu'il se passe en Ukraine pour convaincre, demander de l'aide ou des actions concrètes ;
- 2) Cibler des influenceurs et relais d'opinion en Russie pour tenter de contredire le narratif russe, partager le point de vue ukrainien, envoyer de véritables infos et matériels vidéo ou photo pouvant servir de preuves...

ACTIONS CIBLÉES

Plutôt que de diffuser auprès du plus grand nombre, l'idée est de cibler. Telle grande entreprise présente en Russie ou commerçant avec, telle organisation internationale, tel influenceur, tel politicien européen ou américain, tel artiste : la campagne est préparée, personnalisée, traduite et mise à disposition des membres qui vont la poster sur ces comptes pour les interpeller.



Si vous avez vu des images, des slogans, des argumentaires étayés passés sur les réseaux sociaux de personnalités publiques, il y a de grandes chances que certains aient été préparés par les membres de l'Armée Internet d'Ukraine.

PROCHE DU POUVOIR

Quelles relations avec le pouvoir ukrainien ? Si la majeure partie de cette activité en ligne semble être le fait de simples internautes, le gouvernement du pays n'est jamais très loin. Il faut dire que cette stratégie de communication est aussi celle retenue par le gouvernement de Volodymyr Zelinski. Sur sa page Facebook, son ministre ukrainien de la défense, Oleksiy Reznikov, lançait un appel aux Ukrainiens dès le début de la guerre et les invitait à communiquer les infos officielles gouvernementales en direction des Russes et des journalistes européens. Début mars, le directeur adjoint de l'Agence de cybersécurité ukrainienne, Viktor Zhora, se félicitait devant les journalistes que de nombreux Ukrainiens « s'adressent aux Russes directement par téléphone, par e-mails, par messages ».



PROPOGANDÉ CONTRE PROPAGANDÉ, LES TROLLS RUSSES ONT TROUVÉ À QUI PARLER : 200000 ABONNÉS À LA CHAÎNE TELEGRAM "ARMÉE INTERNET D'UKRAINE" SONT APPELÉS À COMMUNIQUER HORS DE LEURS FRONTIÈRES.



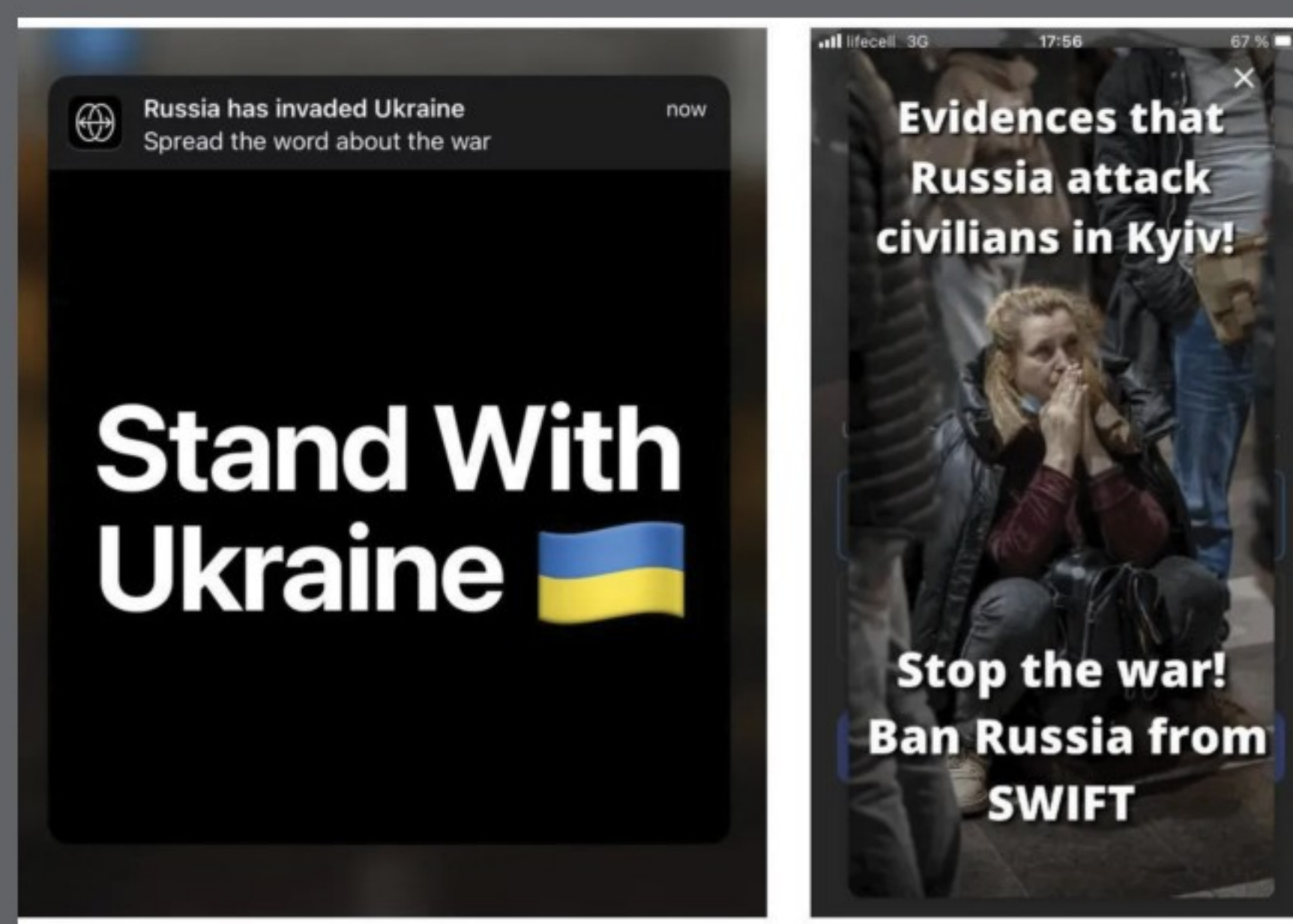
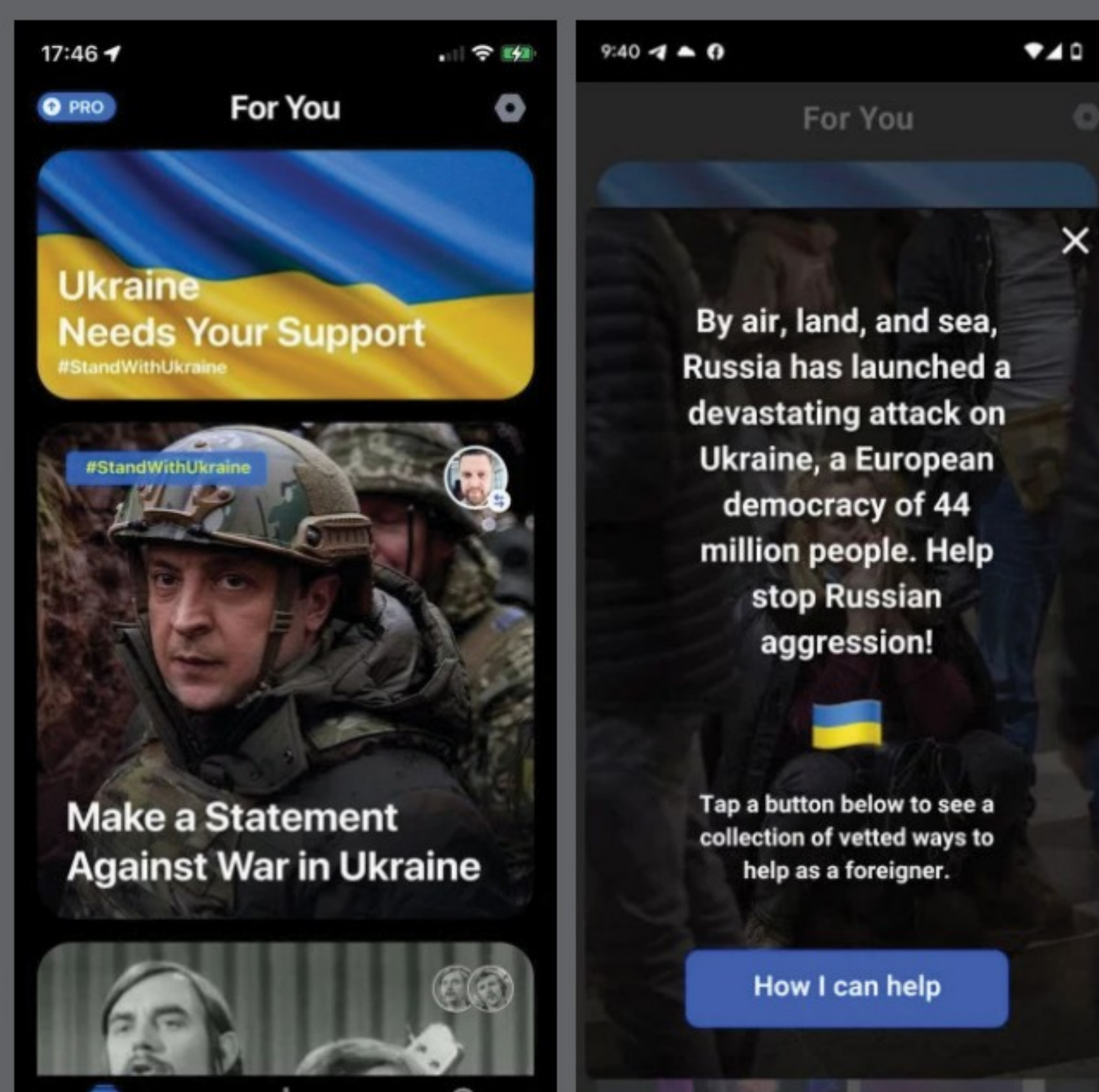


REFACE : l'appli ukrainienne qui passe du deepfake à l'activisme

Nous vous avons déjà parlé de Reface, l'appli ukrainienne spécialisée dans le deepfake récréatif. Ses utilisateurs peuvent prendre leur propre visage ou celui d'un proche pour l'intégrer dans des séquences vidéo, le plus souvent issues de films ou de clips, à la place d'une star par exemple. Reface connaît un vrai succès à l'international et notamment en Russie, où la start-up comptait près de 5,5 millions d'utilisateurs avant la guerre.

TOUCHER LE PUBLIC RUSSE

Depuis le début du conflit, l'équipe de la start-up connaît le même sort que le reste de la population : certains se sont engagés chez les volontaires de l'armée, d'autres ont migré vers l'ouest de l'Ukraine, d'autres ont franchi la frontière. Pour ceux qui restent à Kiev, le temps passe entre mises à l'abri dans le métro, survie quotidienne et entre-aide. Son PDG et co-fondateur, Dima Shvets, s'est rendu compte que tous voulaient d'une manière ou d'une autre soutenir la résistance du pays face à l'envahisseur russe. Alors, pourquoi ne pas utiliser la notoriété de l'appli, en Occident, mais surtout en Russie ?



NOTIFICATIONS

«Reface a lancé une campagne d'information massive et envoyé des notifications push à tous les utilisateurs russes, montrant les preuves d'attaques russes dans nos villes, demandant aux gens de se tenir aux côtés de l'Ukraine et aller aux protestations », explique le dirigeant. « De plus, nous avons ajouté des messages intégrés à l'application aux utilisateurs du monde entier pour soutenir notre pays, et maintenant chaque vidéo réalisée avec notre application a un filigrane avec #standwithukraine et le drapeau ukrainien. »

Reface envoie des notifications à ses millions d'utilisateurs russes pour leur montrer la réalité de la guerre

L'APPLI TOUCHÉE...

«Nous comprenons à quel point cette campagne est risquée et nous les prenons toutes. Nous avons déjà beaucoup de critiques et de rapports 1 étoile de ceux qui n'étaient pas prêts à voir la vérité », a-t-il ajouté. Certains estiment que cette campagne de « downvotes » est orchestrée par les autorités russes pour faire descendre Reface dans le classement et les moteurs de recherche des magasins d'applications. La start-up a appelé ces utilisateurs à contrer cette action en systématisant un vote 5 étoiles.

... MAIS PAS COULÉE

Moscou a mis du temps à se rendre compte que des applis « innocentes » comme Reface s'étaient transformées en armes de communication. Mais contrairement aux réseaux sociaux et médias classiques, difficile pour Roskomnadzor, l'organisme russe de régulation, d'agir rapidement : il ne peut pas bloquer une appli en particulier, mais peut seulement engager des poursuites et réduire leur visibilité sur le Web.

RUNET : INTERNET SOUVERAIN ou DE TYPE NORD-CORÉEN ?



La Russie travaille depuis des années à un projet qui peut nous sembler, à nous Européens, un peu fou : disposer d'un Internet autonome, coupé des autres serveurs mondiaux. Ce projet RuNet est plus qu'un projet, la Russie l'annonce comme opérationnel et a même accéléré les manœuvres depuis 2021. Et pourquoi ne pas s'inspirer de ses aspects les plus positifs ?

D'après le média biélorusse Nexta (documents officiels à l'appui), « *Au plus tard le 11 mars, tous les serveurs et domaines doivent être transférés vers la zone russe. En outre, des données détaillées sur l'infrastructure réseau des sites sont collectées* ». C'est-à-dire que tous les sites administrés en Russie ou souhaitant être intégrés à RuNet doivent avoir migré des clones de leurs sites sur des serveurs russes interconnectés et possédant leur propre architecture de type DNS. L'arsenal juridique est finalisé depuis décembre 2021 et un test de déconnexion en conditions réelles a même été réalisé du 15 juin au 15 juillet dernier.



L'EUROPE DOIT S'EN INSPIRER !

L'Europe, qui a pris l'habitude depuis 70 ans de sous-traiter toute une partie de sa souveraineté militaire, énergétique ou technologique à son allié américain, puis à d'autres puissances, doit se poser la question. Car il n'y a pas que l'ICANN : les pays européens font de plus en plus appel aux géants des télécommunications étrangers, et notamment chinois, pour développer leurs infrastructures réseau filaire et mobile. Il s'agit d'une erreur qui sera payée plus tard si nos états ne mettent pas un terme à cette paresse intellectuelle, financière et technologique. Alors, pourquoi ne pas créer nous aussi un Internet souverain ? Je vous entends pousser des cris d'orfraie.

L'idée n'est pas de créer un Internet européen coupé du monde et sous contrôle étatique, mais de comprendre que la stratégie russe en termes de souveraineté numérique a du sens : prévoir le pire pour ne pas être faible en cas de conflit et pouvoir faire preuve de résilience, mot très à la mode dans la bouche d'Emmanuel Macron ces dernières semaines.

UNE BOUCLE TECHNOLOGIQUE FERMÉE

Un Internet parallèle qui peut donc être activé en cas de mise au ban du Web mondial ou si l'État russe décide lui-même de se déconnecter du «World Wide Web» pour obtenir un contrôle total sur son Internet. Les entreprises russes de télécommunications sont chargées de gérer les moyens techniques de réacheminement de tout le trafic Internet russe vers les noeuds gérés par Roskomnadzor, l'organisme russe de surveillance des télécommunications. Un travail colossal d'infrastructure réseau effectué depuis 2015... mais personne ne sait vraiment s'il résistera à l'épreuve de la réalité. Mais si c'est le cas, le Roskomnadzor sera directement chargé de bloquer les contenus interdits et s'assurera que le trafic entre les utilisateurs russes reste à l'intérieur du pays, et qu'il n'est pas dirigé vers des serveurs à l'étranger, où il pourrait être intercepté. Une muraille infranchissable donc, sauf à demander à y être intégré.

← Tweet



#Russia began active preparations for disconnection from the global Internet

No later than March 11, all servers and domains must be transferred to the #Russian zone. In addition, detailed data on the network infrastructure of the sites is being collected.

LE MÉDIA BIÉLORUSSE NEXTA ANNONCE QUE RUNET ÉTAIT OPÉRATIONNEL ET POUVAIT ÊTRE ACTIVÉ DEPUIS LE 11 MARS.



STARLINK : INTERNET SATELLITAIRE EN CAS DE BLACKOUT

À la demande de l'Ukraine, SpaceX a envoyé des kits de connexion satellitaire à son nouveau réseau StarLink. Un Internet « résilient » et simple à déployer, testé pour la première fois en conditions réelles sur une zone de guerre.

L'accès à Internet est un enjeu majeur lors d'un conflit, pour les administrations comme pour la société civile. Les combats peuvent endommager les infrastructures réseau ou l'un des belligérants peut « éteindre » des zones entières du territoire s'il accède aux centres névralgiques de ce réseau. Une menace plus massive pourrait concerner l'Europe en cas de conflit avec la Russie : une grande partie de notre accès au Web mondial passe par de gigantesques câbles sous-marins reliant notre continent au continent américain. Sectionner ces câbles n'est pas à la portée du premier venu, mais, typiquement, la Russie sait faire et possède les engins qui peuvent descendre et travailler à ces profondeurs.

En attendant de disposer de sa propre architecture souveraine de secours, seuls les fournisseurs d'accès Internet via satellite sont davantage protégés en cas de scénario catastrophe. Mais ils sont ultra-minoritaires en Europe, car chers et nécessitant de lourds investissements.

TEST DE STARLINK EN UKRAINE

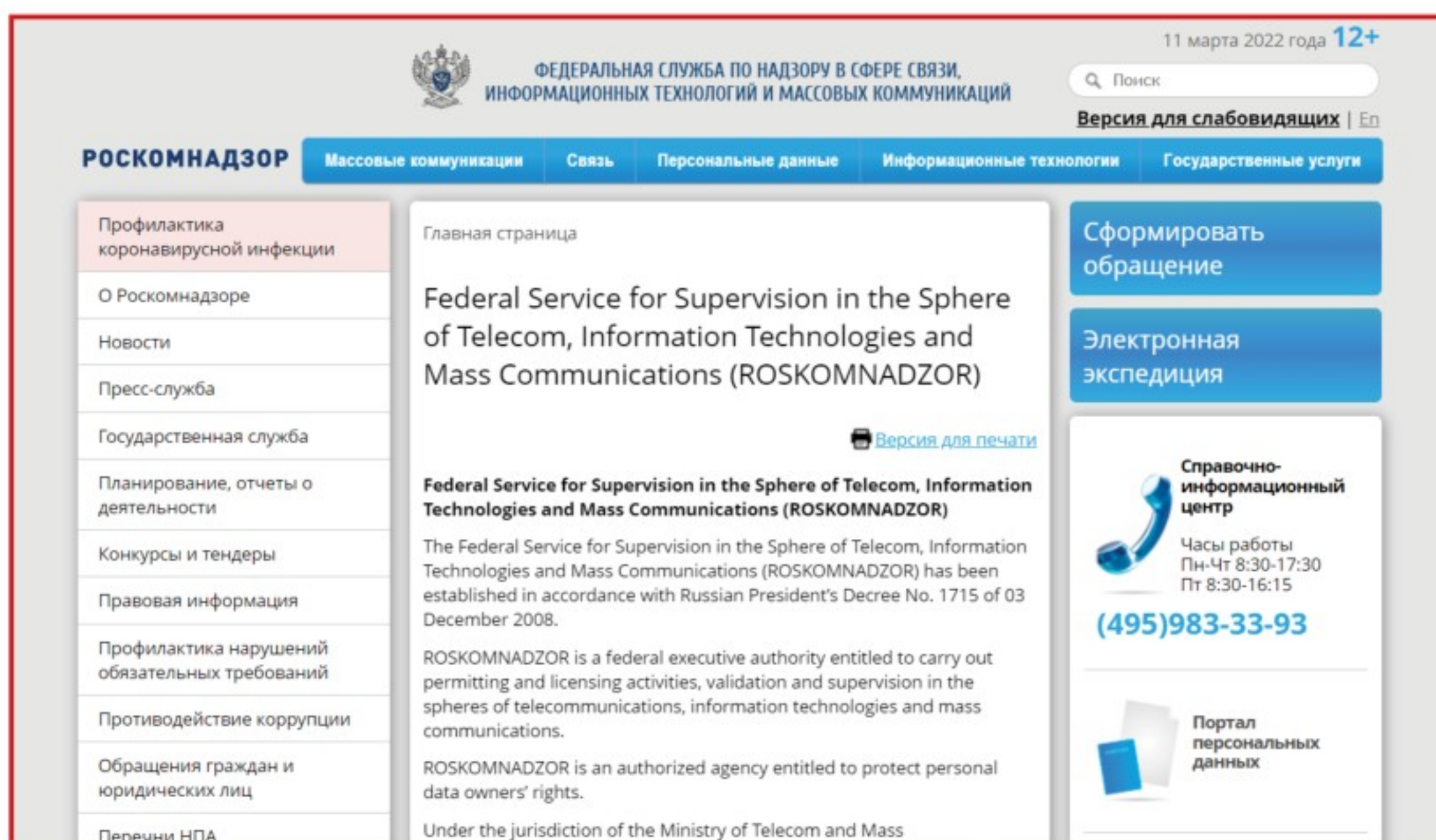
La donne est en train de changer avec l'exemple de la société SpaceX, fondée par Elon Musk. Cette dernière est en train de tester StarLink, son système d'Internet satellitaire nouvelle génération, en Ukraine. Comment cela fonctionne-t-il ? Plutôt qu'un gros satellite de communication, SpaceX parie sur une constellation de microsatsellites de basse altitude pour mailler des territoires plus larges et éviter aussi d'être une cible trop évidente. Surtout, ces myriades satellitaires sont moins onéreuses et plus rapides à envoyer. En 2021, quelques milliers de ces satellites étaient opérationnels. En 2025, SpaceX table sur 25000 unités. Ce qui pose d'autres problèmes : ceux de la pollution et de l'encombrement de notre espace.

INTERNET SUR PLACE OU À EMPORTER

À la demande d'officiels Ukrainiens, SpaceX a d'abord envoyé un premier lot de terminaux StarLink en Ukraine fin février dernier, permettant de maintenir le pays connecté, notamment les services d'urgences. Puis, le 9 mars, un autre lot d'antennes StarLink, ainsi que des batteries Tesla Powerwall ont été acheminées jusqu'en Ukraine pour consolider la connexion Internet. Elon Musk a aussi déclaré que ce lot comprenait « des adaptateurs d'alimentation pour les allume-cigares de voiture, des batteries solaires et des générateurs pour les endroits où l'électricité n'est pas disponible ».



SITÔT DEMANDÉS, SITÔT ENVOYÉS. LES PREMIERS TERMINAUX DE RÉCEPTION STARLINK SONT ARRIVÉS EN UKRAINE FIN FÉVRIER. BIEN SÛR, ELON MUSK COMMUNIQUE SUR CETTE AIDE ET CETTE NOUVEAUTÉ TECHNOLOGIQUE.



NE NOUS MOQUONS PAS, VOICI LE STYLE TRÈS SOVIÉTIQUE DU SITE DE ROSKOMNADZOR, L'ORGANISME EN CHARGE DU CONTRÔLE TOTAL DE RUNET. ÇA DONNE ENVIE.



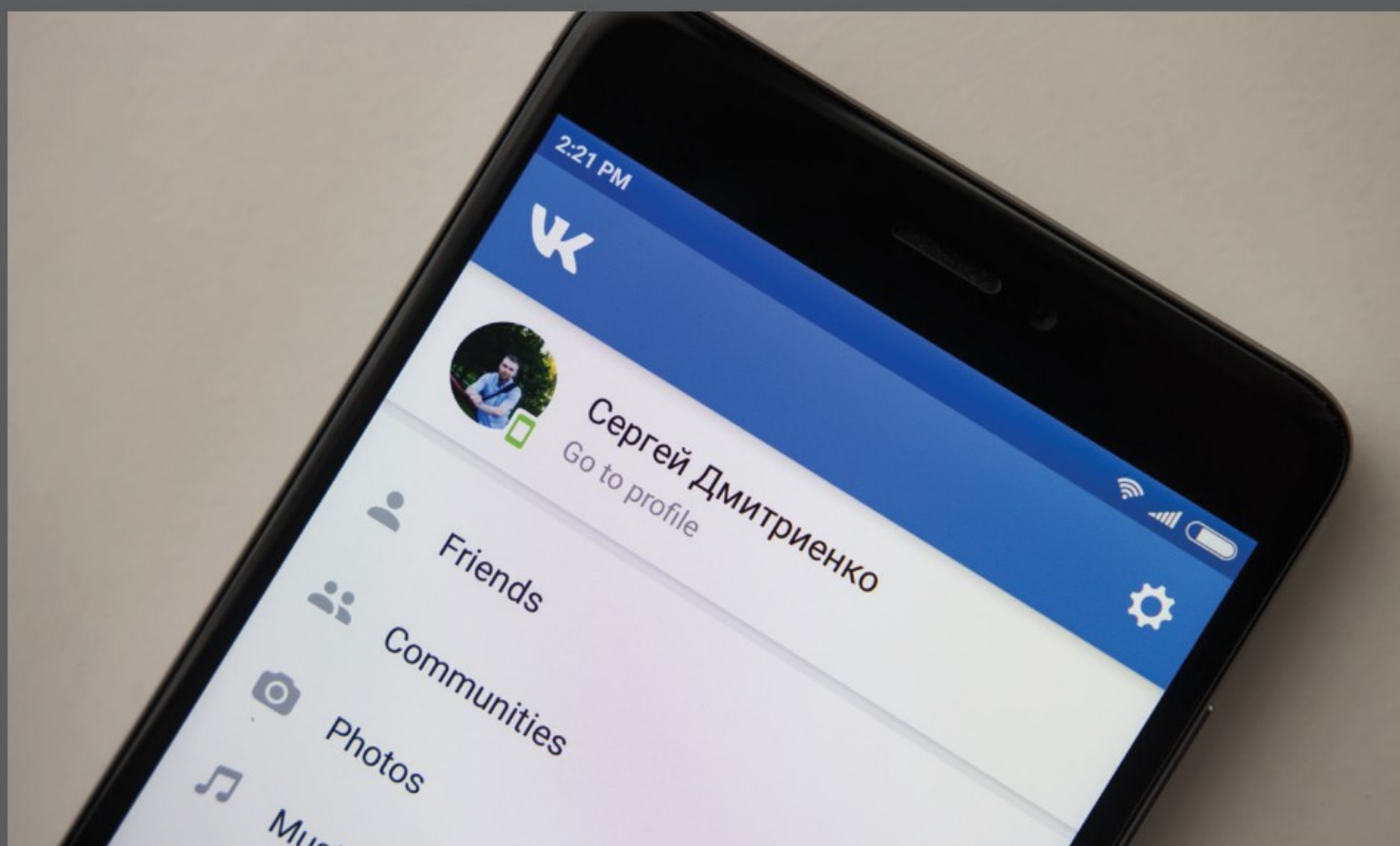
LE PARADIS DE LA CENSURE ET DE L'ARBITRAIRE

Un outil de censure sans équivalent, hormis en Chine, où c'est le pouvoir central qui a droit de vie et de mort sur un site et son contenu, juridiquement et techniquement, sans avoir à en référer à qui que ce soit. Sans oublier que toutes les données des citoyens transiteraient par des serveurs eux aussi gérés par l'État, sans qu'il soit possible pour un Internaute russe de passer par exemple par une solution de sécurisation ou de chiffrement privée non validée et encore moins étrangère. Les gentils citoyens russes évolueraient ainsi au sein d'un gigantesque Intranet, un peu comme dans une entreprise : la direction est capable de savoir qui fait quoi, combien de temps, de dire « toi tu as le droit à tel service, toi non », etc.

VKONTAKTE : Le Facebook russe aux mains de Poutine

Vkontakte, VK pour les intimes, est l'une des grandes réussites Internet russes. Alors qu'aucun réseau social européen n'est parvenu à faire de l'ombre aux géants américains, VK est le plus utilisé en Russie, devançant largement Facebook. Il est le 3e site le plus visité en Russie, après l'américain Google et sa plateforme YouTube.

Créé en 2006 par Pavel Durov, VK était à l'origine un réseau social pour les étudiants et les diplômés du supérieur en Russie, comme Facebook, et il s'est plus tard positionné, comme Facebook encore, en outil de communication plus généraliste pour tous les groupes sociaux et tous les âges. Présentant les mêmes fonctionnalités, il est deux fois plus utilisé en Russie que Facebook (73 % d'utilisateurs russes contre 37 % pour le réseau social américain). VK revendique 100 millions d'utilisateurs mensuels et plus de 15 milliards de messages échangés chaque jour.



HORS DE CONTRÔLE DES USA

Le Kremlin estime que cet Internet souverain est indispensable en cas de conflit mondial, notamment si l'ennemi américain est dans le coup : l'ICANN, l'organisme qui attribue et gère les noms de domaines, est en effet étasunien et donc, selon Moscou, potentiellement sous influence. Andriy Nabok, représentant de l'Ukraine à l'ICANN a d'ailleurs demandé dès le début de la guerre que la Russie soit sanctionnée en déconnectant une partie ou la totalité de ses sites du Web mondial. La direction de l'ICANN a immédiatement réagi en rappelant que « *dans notre rôle de coordinateur technique des identificateurs uniques pour l'Internet, nous prenons des mesures pour nous assurer que le fonctionnement de l'Internet n'est pas politisé, et nous n'avons aucun pouvoir de sanction. En fait, l'ICANN a été créée pour garantir le fonctionnement de l'Internet, et non pour que son rôle de coordination soit utilisé pour l'empêcher de fonctionner* ». Mais ce qui est vrai aujourd'hui le sera-t-il demain ?

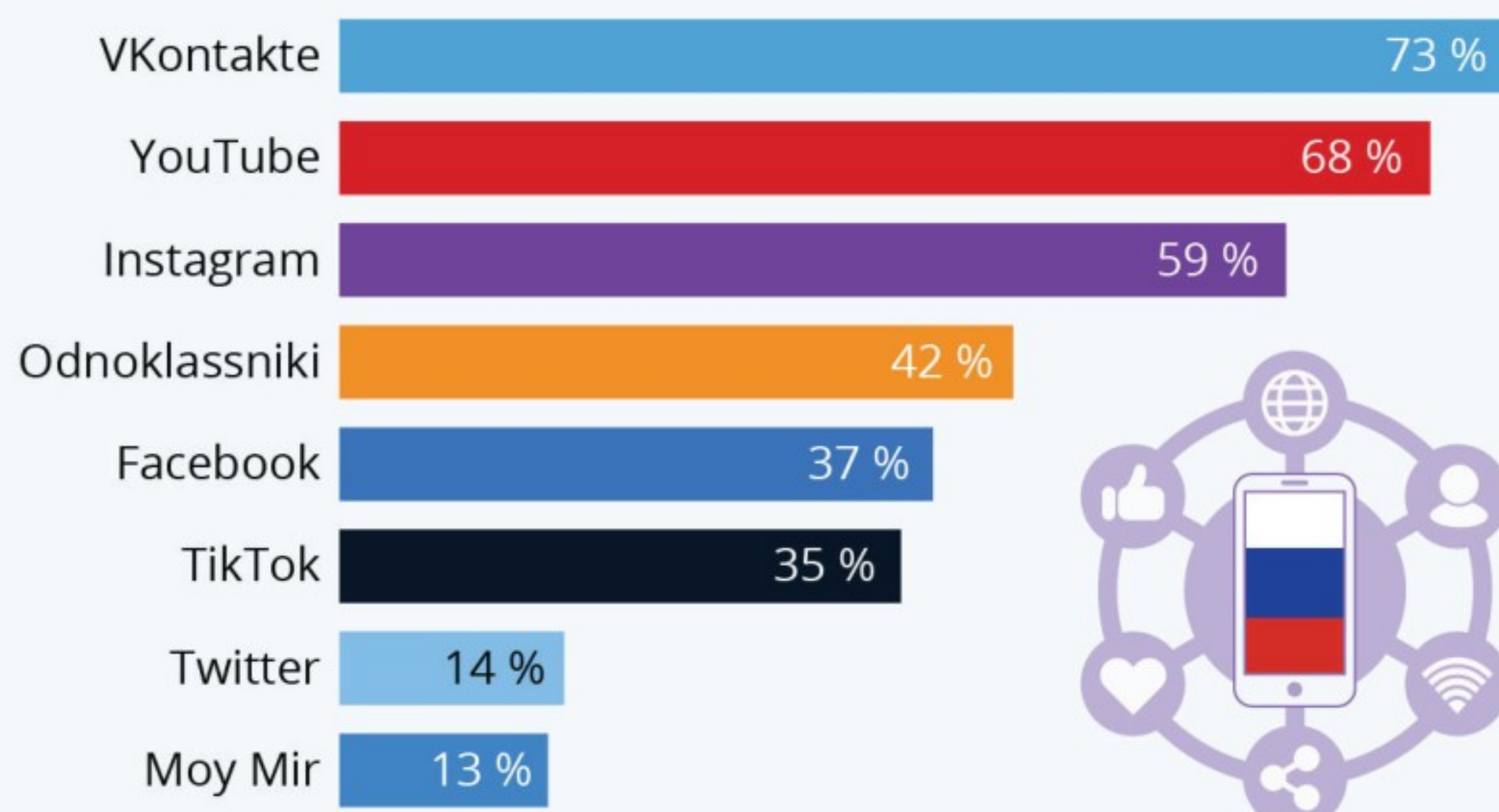
Une muraille infranchissable qui enferme autant qu'elle protège

PLUS DE SOUVERAINETÉ POUR PLUS DE RÉSILIENCE

Pour la Russie, au-delà de la confrontation avec l'Ukraine et le risque de sanctions internationales, l'idée est aussi de garder la main sur ses télécommunications et son écosystème numérique en cas de catastrophe naturelle, de cyberattaque massive, de pandémie ou de tout autre événement cataclysmique. La loi sur la souveraineté d'Internet mise en place l'année dernière accorde un pouvoir de déconnexion sans nécessité de justification précise, au nom de la «sécurité nationale», une notion certes extrêmement vague.

Quels réseaux sociaux utilisent les Russes ?

Réseaux sociaux avec la plus grande part d'utilisateurs en Russie en 2021, en % *



* Base : 2 049 répondants (18 à 64 ans) interrogés entre janvier et décembre 2021.
Source : Statista Global Consumer Survey

LE CAPITAINE S'EXILE

Il a longtemps été vu comme un réseau social fun, jeune et un peu rebelle. Mais dès 2014, son créateur a quitté la Russie après avoir été «contraint» (cela est discuté) de céder son groupe à un proche de Vladimir Poutine. Il évite depuis son pays d'origine et a fondé la populaire messagerie cryptée Telegram. Et en décembre 2021, les liens avec le Kremlin ont été à nouveau resserrés : VK a été racheté par Sogaz, une entreprise publique d'assurance russe appartenant au groupe Gazprom Media, la branche média et communication du groupe Gazprom, sous le contrôle des autorités russes. Vladimir Kirienko, le fils de Sergueï Kirienko, chef adjoint de l'administration présidentielle (!), a hérité du poste de PDG.

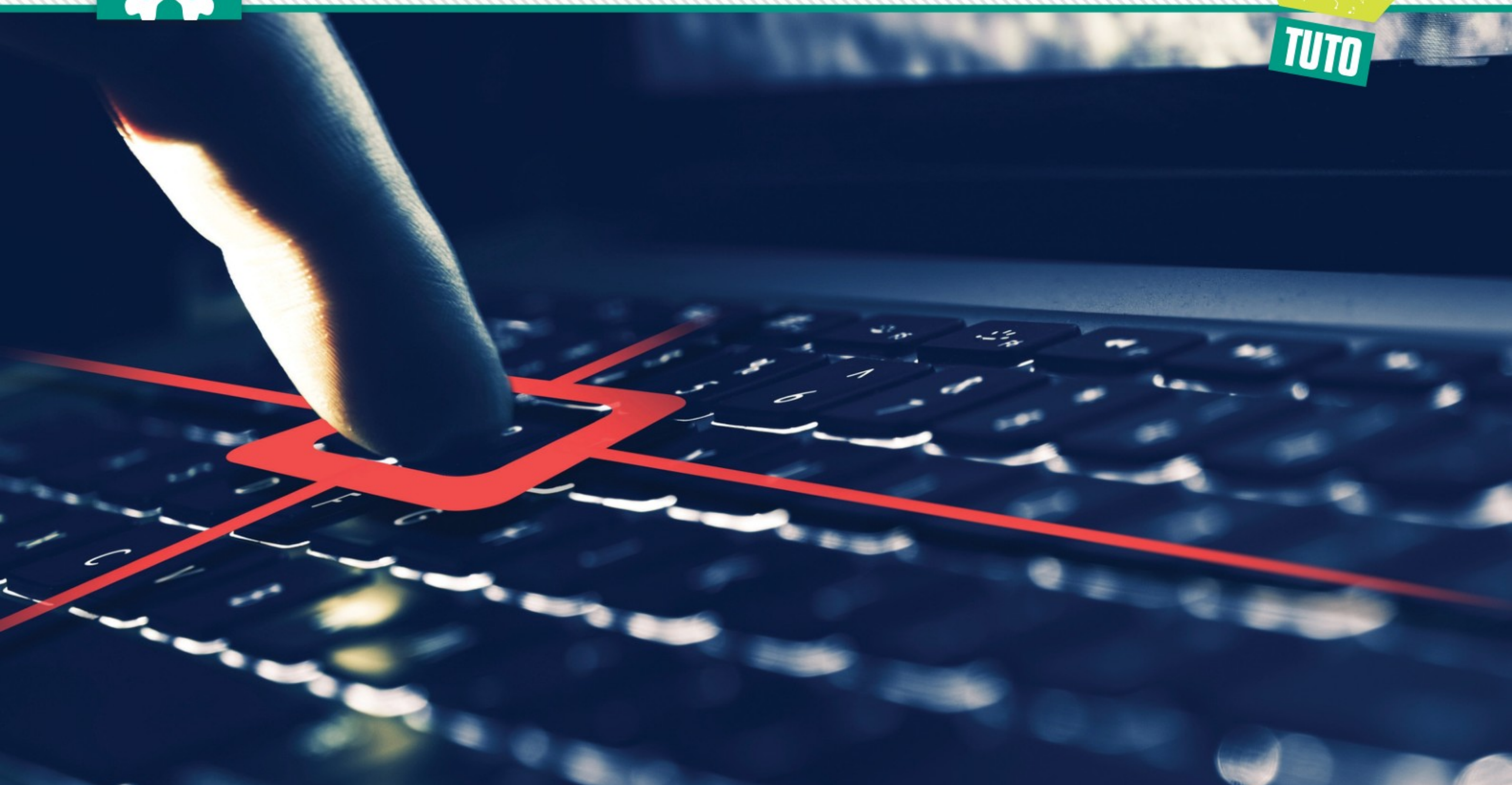


statista

VKONTAKTE À NOUVEAU AUTORISÉ EN UKRAINE

En mai 2017, l'Ukraine ordonnait le blocage de VKontakte sur son territoire suite à l'annexion de la Crimée en 2014 et au conflit qui l'oppose à la Russie à l'Est de son territoire depuis cette même année. Le moteur de recherche Yandex est aussi concerné par cette décision.

Le 1^{er} mars dernier, le ministre de l'intérieur ukrainien a de nouveau autorisé l'accès à VKontakte pour ses concitoyens. L'objectif : leur permettre de participer aux échanges sur le territoire russe et d'alimenter en infos et en avis le réseau social pour toucher la population russe en y publiant « *un maximum de photographies, de vidéos et de documents* », notamment concernant les soldats russes faits prisonniers et les dégâts causés par l'armée russe.



SURVEILLEZ CHAQUE MOT GRÂCE À UN KEYLOGGER

Il n'y a plus de secret. Les keyloggers enregistrent toutes les frappes, petites ou grandes, sur les claviers des ordinateurs.

Vous voulez savoir tout ce qu'une personne tape sur son clavier ? C'est le but d'un keylogger. Certains ont bien compris que ces logiciels espions étaient la clé pour pirater vos comptes en banque en récupérant vos mots de passe. Quelques patrons les apprécient également pour surveiller la productivité de leurs employés ainsi que la légalité des activités numériques opérées sur un lieu de travail. Notamment pour être certains qu'ils n'envoient pas de messages personnels (ou d'informations secrètes sur l'entreprise). D'autant plus que ces enregistreurs de frappe jouent de plus en plus les petits malins : ils peuvent filtrer le type de données récupérées, ou les sites web sur lesquels des mots sont entrés.

UN OUTIL, DIFFÉRENTES FORMES

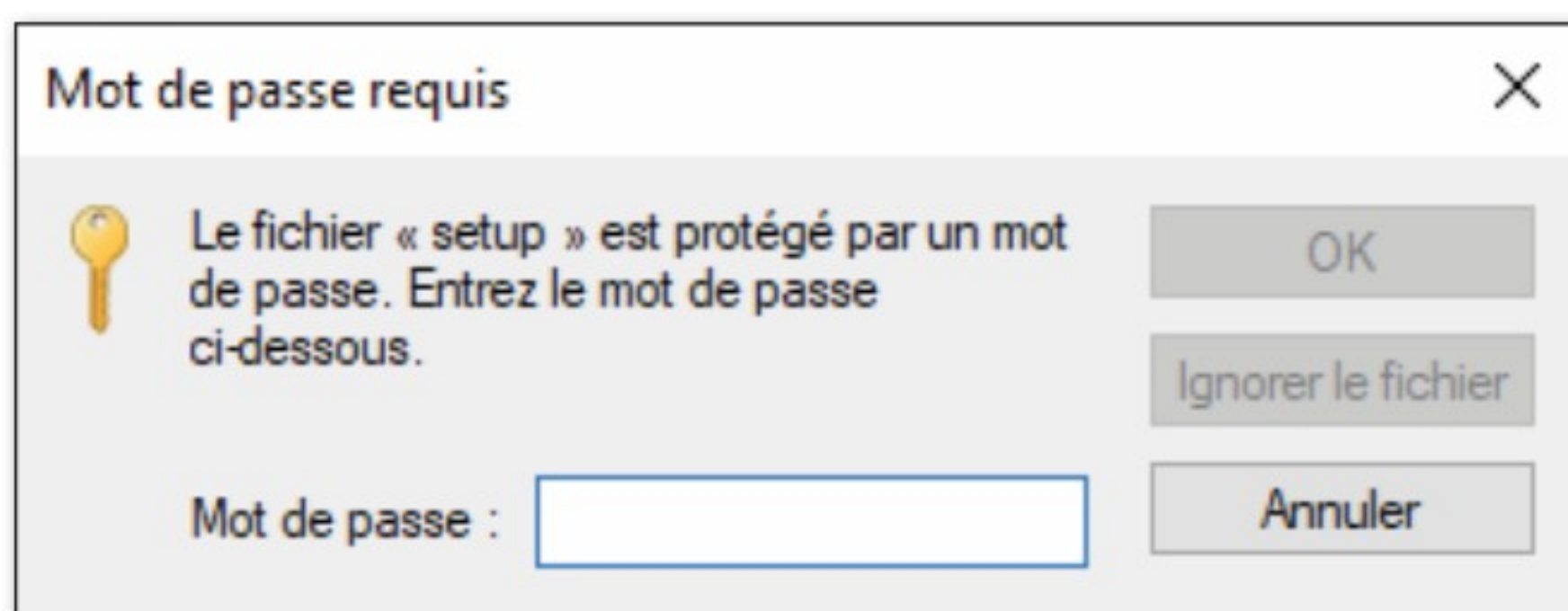
Les keyloggers se présentent sous différents aspects. Tout d'abord, la version logicielle. Soit en version hooking, via un programme qui utilise Windows pour surveiller toutes les frappes (et même les mots de passe automatiques). C'est souvent la solution choisie par les escrocs puisqu'il suffit de l'intégrer dans un exécutable. Il existe aussi en version malware liée au système central, capable d'intercepter directement les informations provenant du clavier. Il est alors indétectable pour l'utilisateur (mais il est inefficace sur les mots de passe automatique). Enfin, la version matérielle, que tout le monde a déjà vue dans les films d'espions ou d'arnaque. Un dispositif placé entre le clavier et l'ordinateur se charge alors de capturer le nécessaire.



CONFIGUREZ UN KEYLOGGER GRATUIT

01 > INSTALLER LE LOGICIEL

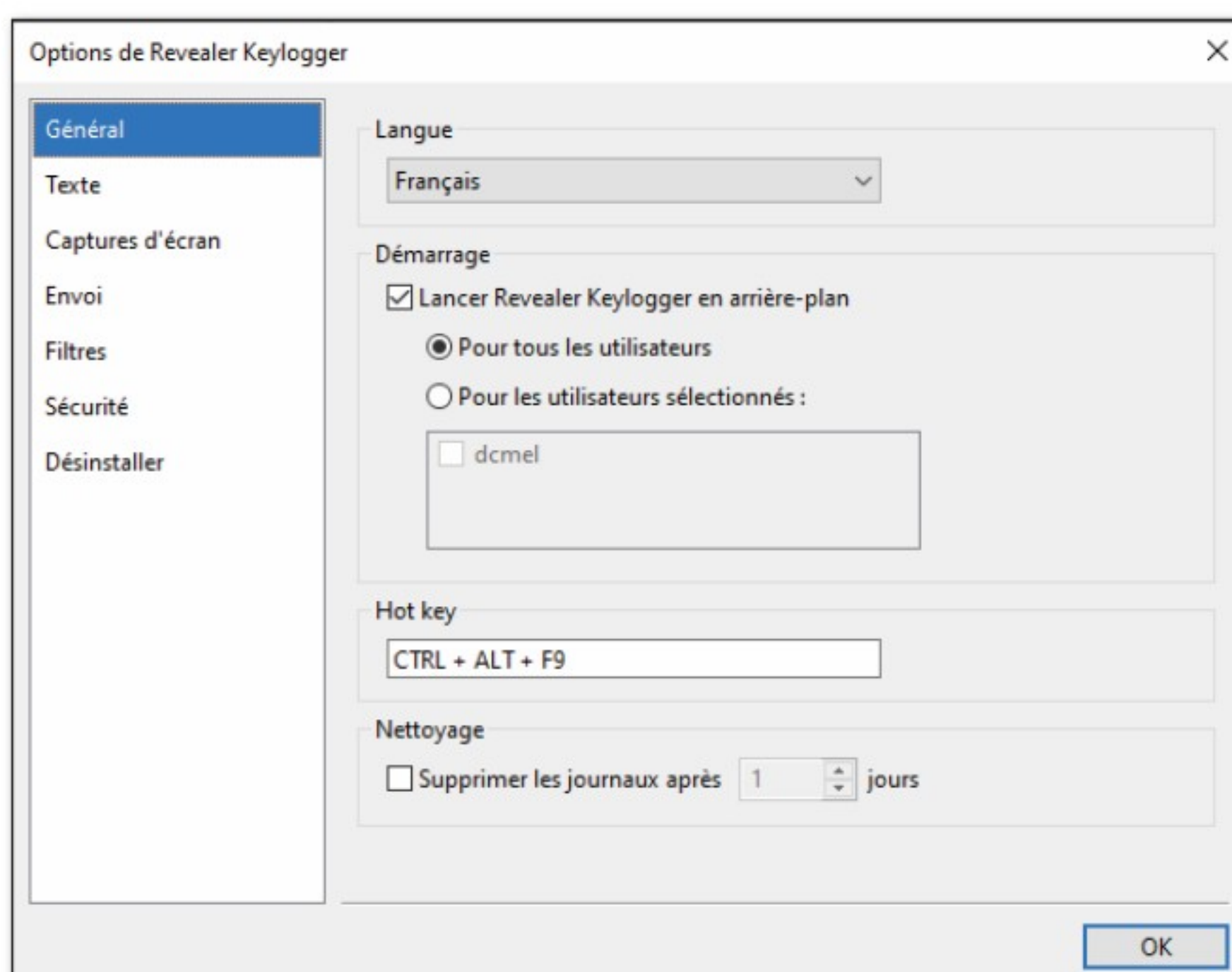
Pour avoir accès à l'exécutable vous permettant de télécharger Revealer Keylogger, vous devrez entrer un mot de passe. Celui-ci est indiqué dans le nom du fichier de téléchargement, mais si vous l'avez oublié, il est très simple, c'est **123**.



02 > DÉFINIR LANGUE ET MOT DE PASSE

Une fois le programme ouvert, cliquez sur la petite roue crantée, en haut à droite, pour avoir accès aux options. Sur l'onglet **Général**, vous pourrez **Choisir sa langue** (par défaut ce sera celle de votre système). Vous pourrez aussi décider s'il se lance pour tous les utilisateurs ou seulement pour certains (si vous avez plusieurs profils installés sur votre ordinateur).

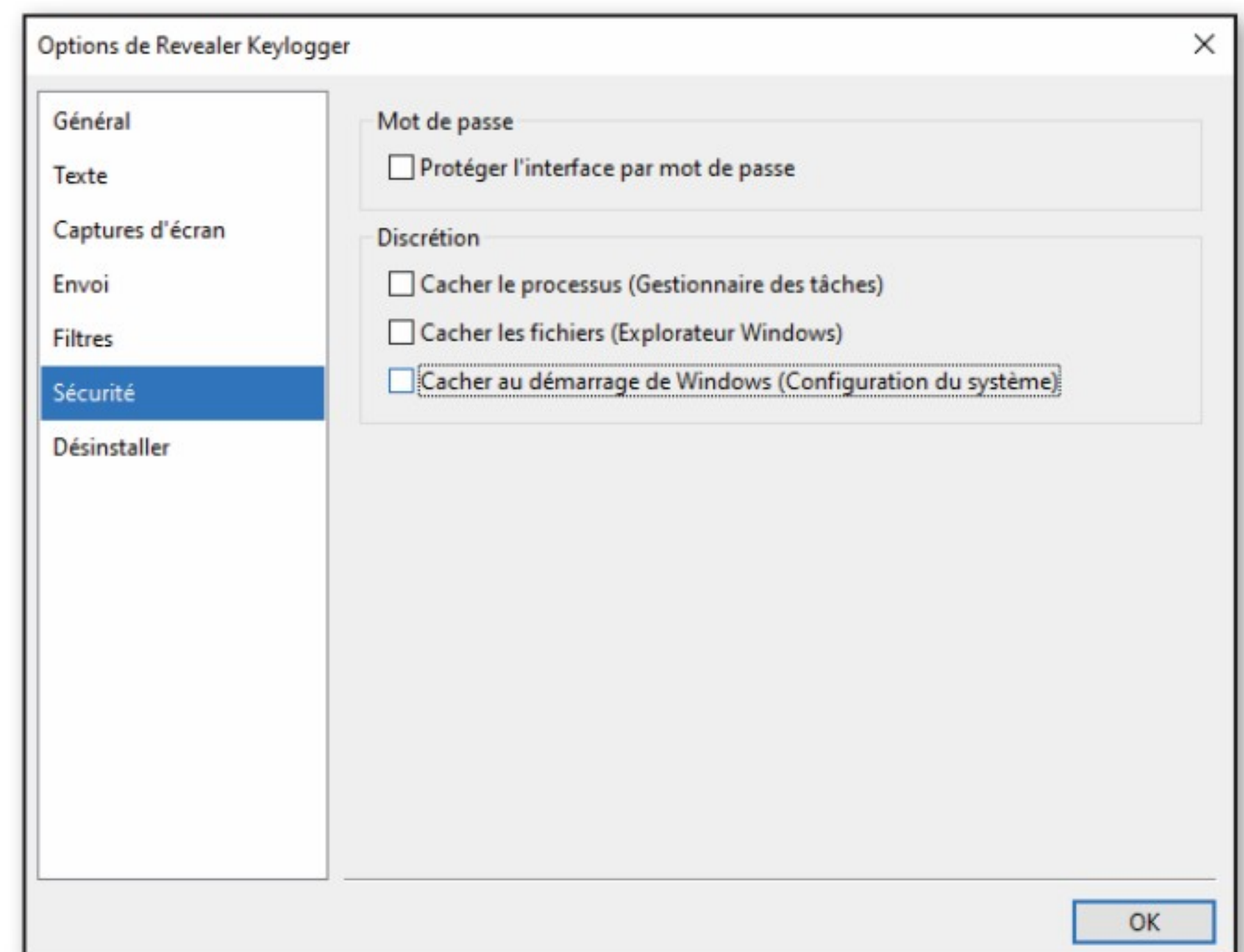
Le **Hotkey**, c'est le code clavier qui vous permettra de faire apparaître Revealer Keylogger quand il est caché, et donc d'avoir accès aux journaux.



03 > PROTÉGER PAR UN MOT DE PASSE

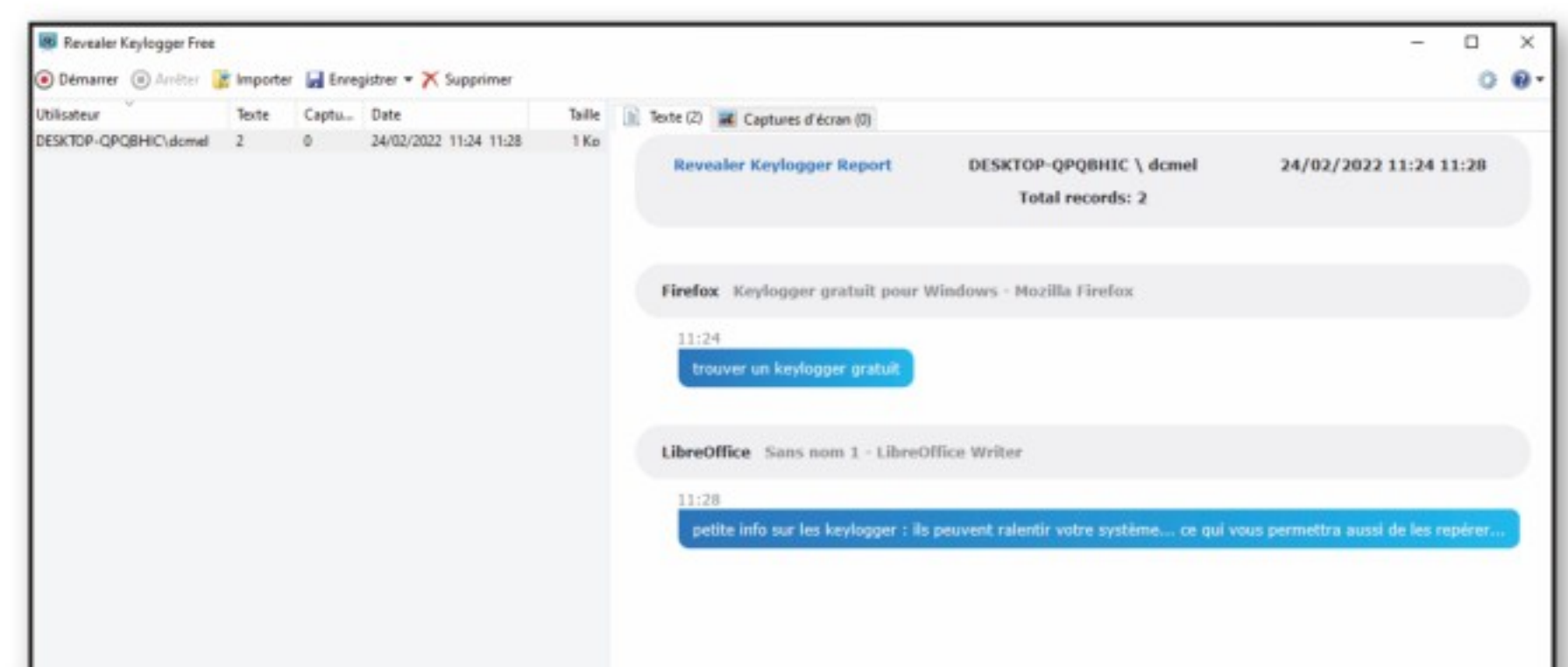
La plupart des options ne sont pas accessibles en version gratuite. C'est notamment le cas pour les captures d'écran, l'envoi des journaux d'enregistrement par mail ou les filtres. De même, vous ne pourrez pas cacher le processus (ce qui vous permet de rester dans la légalité, car enregistrer les actes d'une autre

personne sans son consentement est passible d'une amende et d'une peine de prison). Par contre, vous pourrez protéger l'interface par mot de passe, pour empêcher sa désactivation, par exemple.



04 > ENREGISTRER ET OBSERVER

Une fois l'application paramétrée, cliquez sur **Démarrer** pour lancer un enregistrement de frappe de clavier. En cliquant sur un utilisateur dans la fenêtre de gauche, vous accéderez à tout ce qu'il a écrit, ainsi que dans quel logiciel. Le tout apparaîtra de manière très lisible dans la colonne de droite, avec un horodatage relativement précis.





ANALYSEZ VOTRE CONFIGURATION

AIDA64 analyse en détail les composants matériels de votre ordinateur, votre système d'exploitation, et vos logiciels. Un outil précieux pour la détection et la réparation d'éventuels problèmes.



Dès son lancement, AIDA64 décortique votre PC : matériel, logiciels, pilotes, BIOS, Registre, il inventorie et analyse tout. Grâce à ses benchmarks intégrés, il va ensuite pouvoir jauger la puissance de votre configuration, et surtout réaliser un « stress test », consistant à faire tourner à fond l'ordinateur, le poussant dans ses derniers retranchements. Le but est de faire apparaître d'éventuelles faiblesses (surchauffe, voltage inadéquat, logiciel mal installé, etc.). Si un composant s'avère défaillant, l'identification précise de son type et de son modèle vous permettra de trouver facilement la pièce de remplacement. Notez que AIDA64 est payant (quelques dizaines d'euros), mais sa version d'essai

de 30 jours permet de l'utiliser sans bourse délier pour un besoin ponctuel.

AIDA64 propose 30 jours d'essai gratuit et permet aux particuliers d'accéder ainsi à un outil pro et puissant.

PREMIERS PAS AVEC AIDA64

PRATIQUE



01 > TÉLÉCHARGER

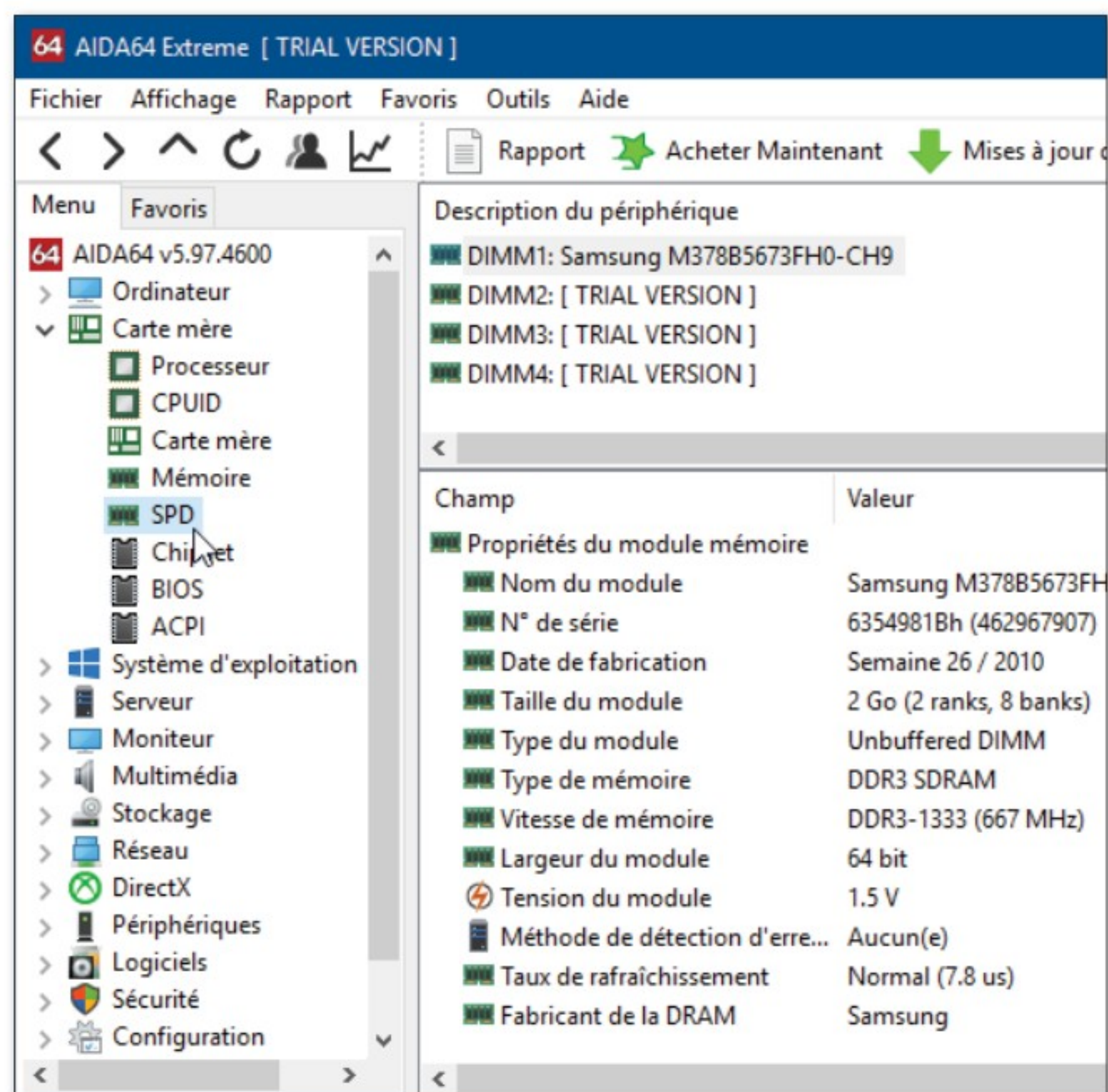
Sur le site de l'éditeur, choisissez **Downloads**, en haut de la page, pour accéder au téléchargement. Optez pour

▼ Downloads				
	Version	Release Date	Size	
AIDA64 Extreme	6.25.5400	Apr 07, 2020	45.4 MB	Buy now Download
Trial version, self-installing EXE package				
AIDA64 Extreme	6.25.5400	Apr 07, 2020	48.97 MB	Buy now Download
Trial version, portable ZIP package				
AIDA64 Engineer	6.25.5400	Apr 07, 2020	44.58 MB	Buy now Download
Trial version, self-installing EXE package				
AIDA64 Engineer	6.25.5400	Apr 07, 2020	48.14 MB	Buy now Download
Trial version, portable ZIP package				
AIDA64 Business	6.25.5400	Apr 07, 2020	48.53 MB	Buy now Download
Trial version, portable ZIP package				
AIDA64 Network Audit	6.25.5400	Apr 07, 2020	15.66 MB	Buy now Download
Trial version, portable ZIP package				
AIDA64 for Android	1.72	May 12, 2020	8.9 MB	Download
Download the app from Google Play				
AIDA64 for iOS	1.37	Jul 09, 2020	24.6 MB	Download
Download the app from App Store				
AIDA64 for Sailfish	2.0.6	Mar 12, 2020	225 KB	Download
Download the app from Jolla Store				
AIDA64 for Ubuntu Touch	1.0.1	Jul 23, 2016	312 KB	Download
Download the app from Ubuntu Store				
AIDA64 for Windows Phone	2.1.0.0	May 03, 2017	21.4 MB	Download
Download the app from Windows Store				

l'édition **AIDA 64 Extreme**, en version installable classique (**EXE**), ou en version portable (**ZIP**) que vous pouvez mettre sur une clé USB : pratique si vous devez aller dépanner le PC d'un ami.

02 > LANCER LE LOGICIEL

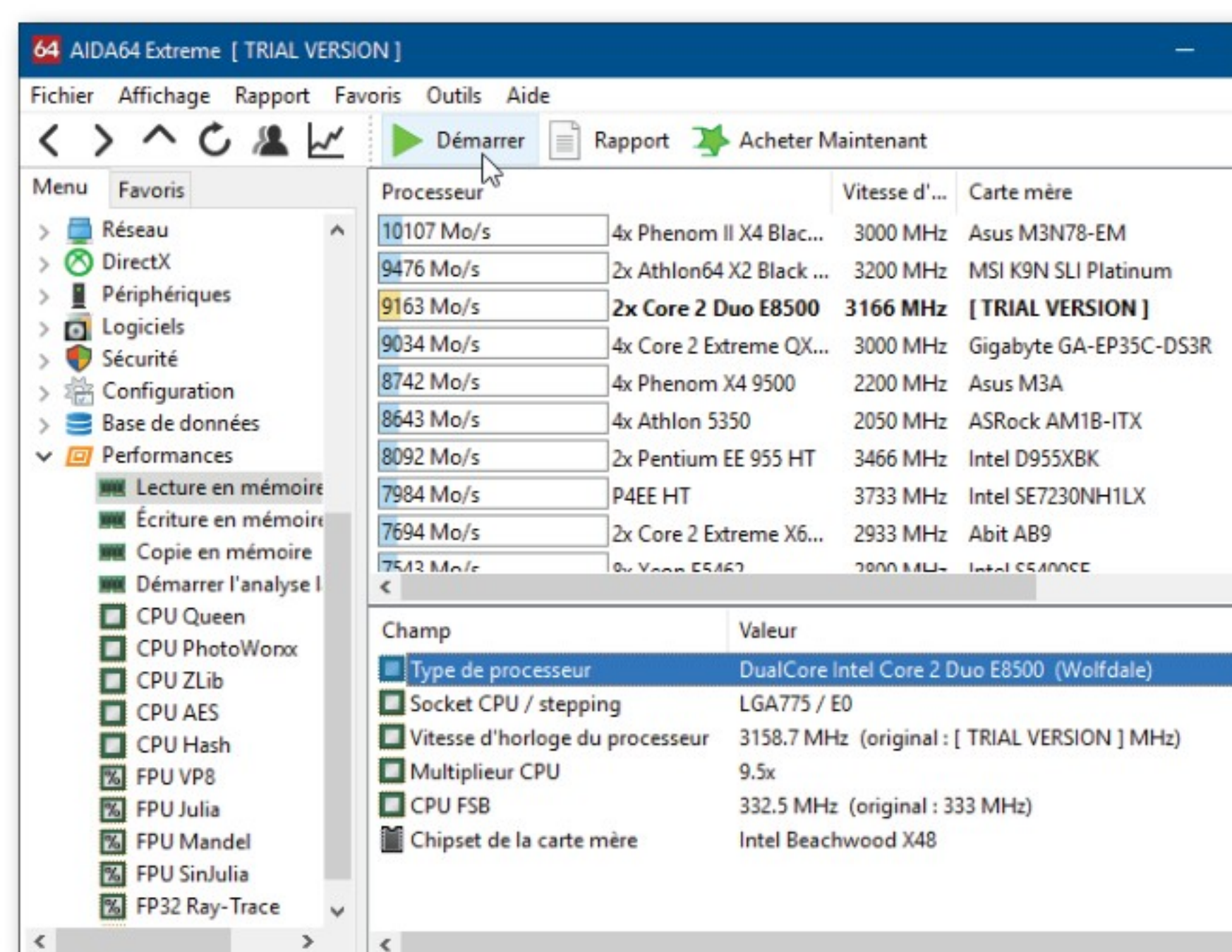
Décompressez l'archive Zip téléchargée (clic droit, **Extraire tout**), puis double-cliquez sur **aida64.exe** pour lancer le logiciel. Explorez ensuite les diverses catégories et



sous-catégories proposées dans la colonne de gauche pour tout savoir sur votre ordinateur.

03 > MESURER LES PERFORMANCES

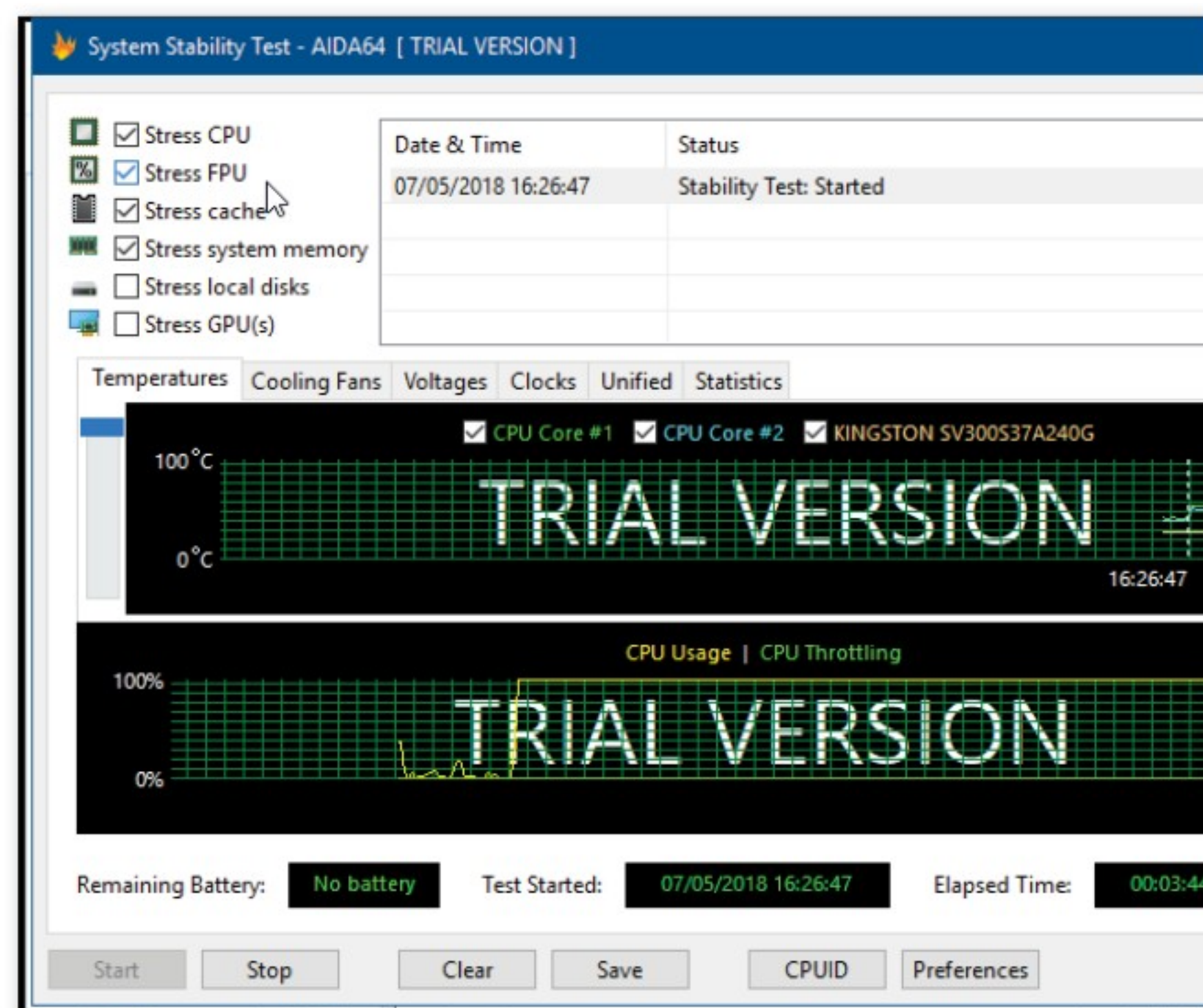
Dans la catégorie **Performances**, vous trouvez différents outils pour tester les performances de votre processeur



(cliquez sur **Démarrer**, en haut)). Pour chaque benchmark, vous avez des mesures effectuées sur d'autres composants que les vôtres pour comparer.

04 > VÉRIFIER LA STABILITÉ

Dans le menu **Outils**, choisissez **Test de stabilité système**. Ce « stress test » va faire fonctionner vos



processeur, mémoire vive, carte graphique et disque dur à 100 % dans le but de vérifier le bon fonctionnement des ventilateurs, de contrôler la température, de mesurer le voltage ou les erreurs d'écriture sur l'espace de stockage.



RÉCUPÉREZ TOUTES LES ADRESSES MAIL D'UN DOMAINE

Vous désirez récupérer toutes les adresses d'un domaine Internet ? EmailHarvester automatise la tâche et recherche des e-mails en utilisant une dizaine de ressources et moteurs de recherche.

EmailHarvester est une sorte de web crawler, il explore automatiquement Internet à la recherche de contenu ciblé. Souvent utilisé par les spammeurs pour collecter des adresses à qui envoyer du pourriel, ce type de logiciel peut aussi être utilisé pour des tâches plus nobles. Par exemple : récupérer les adresses d'une société pour l'envoi de CV ou pour trouver une personne particulière.

LES MOTEURS DE RECHERCHE SONDÉS

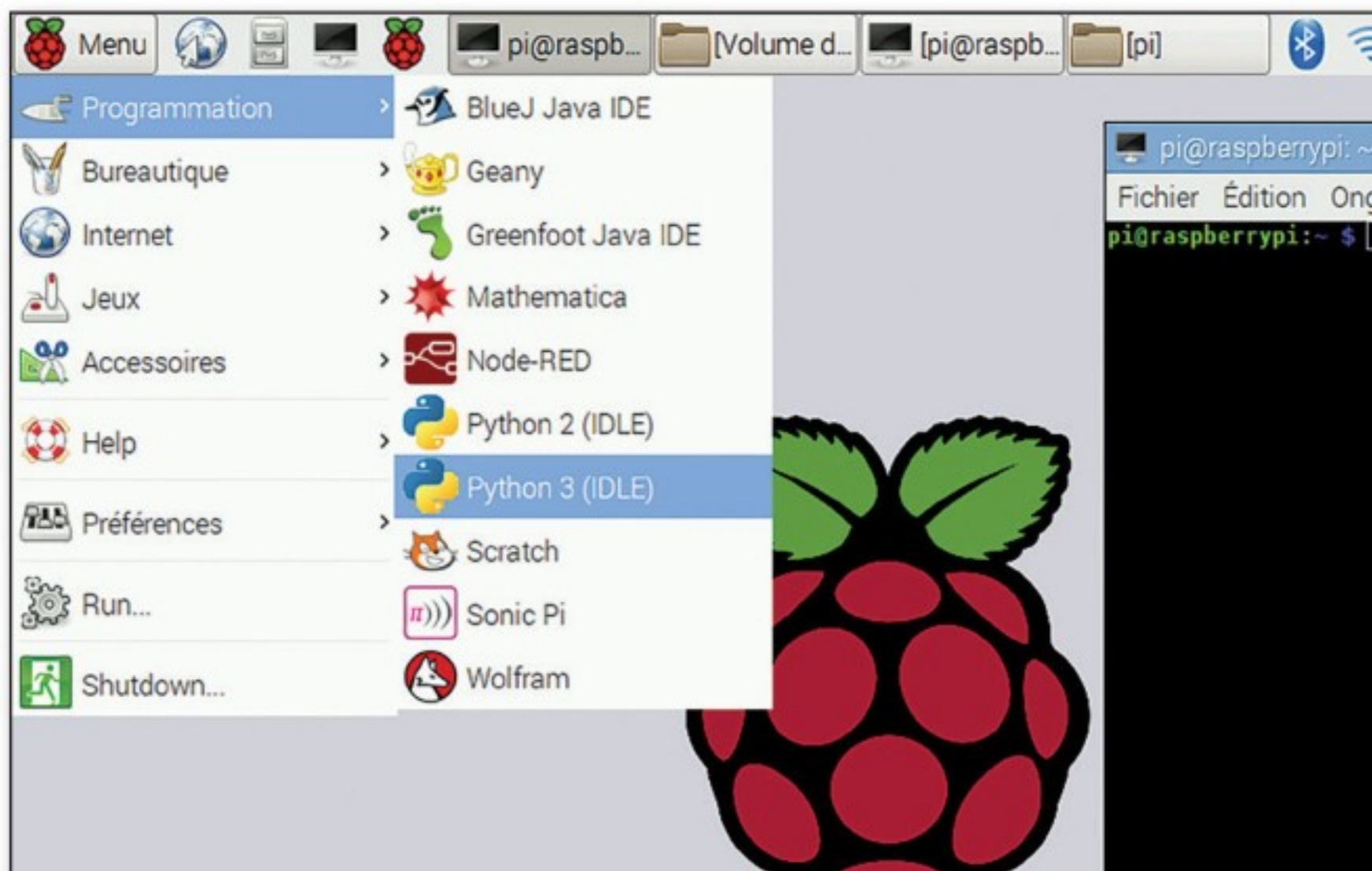
Ce type d'outil peut aussi être utilisé pour du footprinting avec Maltego. Une technique qui consiste à glaner le plus d'infos sur un individu, une société ou un site et de dresser une liste de toutes les entités auxquelles ils sont rattachés. Vous pouvez aussi tester votre propre nom de domaine pour vous prémunir du spam ou du mail bombing. EmailHarvester va chercher des adresses e-mail laissées «en clair» sur le Net en questionnant les moteurs de recherche les plus connus (Google, Bing, Yahoo...) ainsi que les moteurs de Twitter, Reddit ou Instagram.



COMMENCER LA MOISSON

01 > L'UTILISER SOUS LINUX

Sur un Raspberry Pi, nous utilisons ici Raspbian, une version spéciale de la distribution Linux Debian. Lancez un terminal et tapez : **sudo apt-get update && upgrade** Vous mettez alors à jour vos paquets et le système puis : **git clone https://github.com/maldevel/EmailHarvester**. Cela copie les fichiers dans un dossier **EmailHarvester**.



changer le code Python pour ajouter vos propres moteurs de recherche...

```

Fichier Édition Onglets Aide
pi@raspberrypi:~/EmailHarvester $ ./EmailHarvester.py -d idpresse.c
[+] User-Agent in use: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
01 Firefox/40.1
[+] Searching everywhere
[+] Searching in Dogpile: 11 results
[+] Searching in Dogpile: 21 results
[+] Searching in Dogpile: 31 results
[+] Searching in Dogpile: 41 results
[+] Searching in Dogpile: 51 results
[+] Searching in Dogpile: 61 results
[+] Searching in Dogpile: 71 results
[+] Searching in Dogpile: 81 results
[+] Searching in Dogpile: 91 results
[+] Searching in Dogpile: 101 results
[+] Searching in Google+: 100 results
[+] Searching in Youtube
[+] Searching in Yahoo + Youtube: 101 results
[+] Searching in Bing + Youtube: 50 results
[+] Searching in Bing + Youtube: 100 results
[+] Searching in Google + Youtube: 100 results
[+] Searching in Baidu + Youtube: 10 results
[+] Searching in Baidu + Youtube: 20 results
[+] Searching in Baidu + Youtube: 30 results
[+] Searching in Baidu + Youtube: 40 results
  
```

02 > INSTALLER

Pointez vers ce dossier avec **cd EmailHarvester**. Il faut ensuite ajouter les librairies nécessaires pour la version de Python que nous devons utiliser : **python3 -m pip install -r requirements.txt --user**. Rendez le script exécutable avec :
chmod +x EmailHarvester.py

```

Fichier Édition Onglets Aide
pi@raspberrypi:~/EmailHarvester $ python3 -m pip install -r re
ser
Downloading/unpacking termcolor (from -r requirements.txt (lin
  Downloading termcolor-1.1.0.tar.gz
  Running setup.py (path:/tmp/pip-build-vue396pz/termcolor/set
  r package termcolor

Requirement already satisfied (use --upgrade to upgrade): colo
python3/dist-packages (from -r requirements.txt (line 2))
Requirement already satisfied (use --upgrade to upgrade): requ
python3/dist-packages (from -r requirements.txt (line 3))
Downloading/unpacking validators (from -r requirements.txt (li
  Downloading validators-0.10.3.tar.gz
  Running setup.py (path:/tmp/pip-build-vue396pz/validators/se
  or package validators

warning: no previously-included files matching '*.pyc' fou
'tests'
warning: no previously-included files matching '*.pyc' fou
'docs'
no previously-included directories found matching 'docs/_b
warning: no previously-included files found matching 'docs
Requirement already satisfied (use --upgrade to upgrade): six>
/python3/dist-packages (from validators->-r requirements.txt (
  
```

03 > TAPER LES COMMANDES

Lancez cette commande : **./EmailHarvester.py -d idpresse.com -e all**

Cette dernière va chercher les adresses du domaine idpresse.com sur tous les moteurs de recherche connus par EmailHarvester. Vous pouvez changer cette commande :

./EmailHarvester.py -d toyota.fr -e google. Libre à vous de

04 > ALLER PLUS LOIN

Email Harvester ne va pas assez loin ?

Vous voudriez récupérer d'autres informations automatiquement à partir du Web ? Scrapy est un framework, téléchargeable depuis ce lien :

https://scrapy.org, qui permet de créer des web crawlers sur-mesure. Pour récupérer toutes sortes d'informations (les liens d'une page Web, le contenu éditorial...).

```

$ pip install scrapy
$ cat > myspider.py <<EOF
import scrapy

class BlogSpider(scrapy.Spider):
    name = 'blogspider'
    start_urls = ['https://blog.scrapinghub.com']

    def parse(self, response):
        for title in response.css('h2.entry-title'):
            yield {'title': title.css('a ::text')}

        for next_page in response.css('div.prev-pc
            yield response.follow(next_page, self.
EOF
$ scrapy runspider myspider.py
  
```





GARDER SON HISTORIQUE EN NAVIGATION PRIVÉE

PRATIQUE



Le mode navigation privée de Chrome ne laisse pas de traces sur votre PC, mais il vous prive de l'historique, parfois bien pratique. Sauf si vous installez l'extension Off the record.



INFOS [Off the record history]

Où le trouver ? [<https://goo.gl/vRYDOR>]

Difficulté :

Off The Record History 0.1.2

Track your browsing history in incognito mode. Self-destructs history

Détails

☒ Autoriser en mode navigation privée

Avertissement : Google Chrome ne peut pas empêcher les extensions d'historique de navigation. Pour désactiver cette extension en mode navigation privée, désélectionnez-la.

01 > ACTIVER L'EXTENSION

Après avoir installé l'extension, cliquez sur les trois points en haut à droite de votre navigateur. Cliquez sur **Plus d'outils** et **Extensions**. Cherchez **Off the record** et cochez **Autoriser en mode navigation privée**. Sans cela, l'extension ne marchera pas.

Off the record history

Recently closed

Full history

Facebook - Connexion ou inscription	10
facebook - Recherche Google	10
Gmail	10
Gmail - La messagerie avec espace de stockage gratuit de ...	10

02 > CONSULTER L'HISTORIQUE

Pour voir votre historique, cliquez sur l'icône de l'extension. Vous aurez accès à vos onglets fermés (**Recently closed**) et votre historique depuis le début de la session privée (**Full History**). Une fois la fenêtre de navigation fermée, votre historique disparaît définitivement.

GÉNÉRER DES EMAILS À USAGE UNIQUE

PRATIQUE



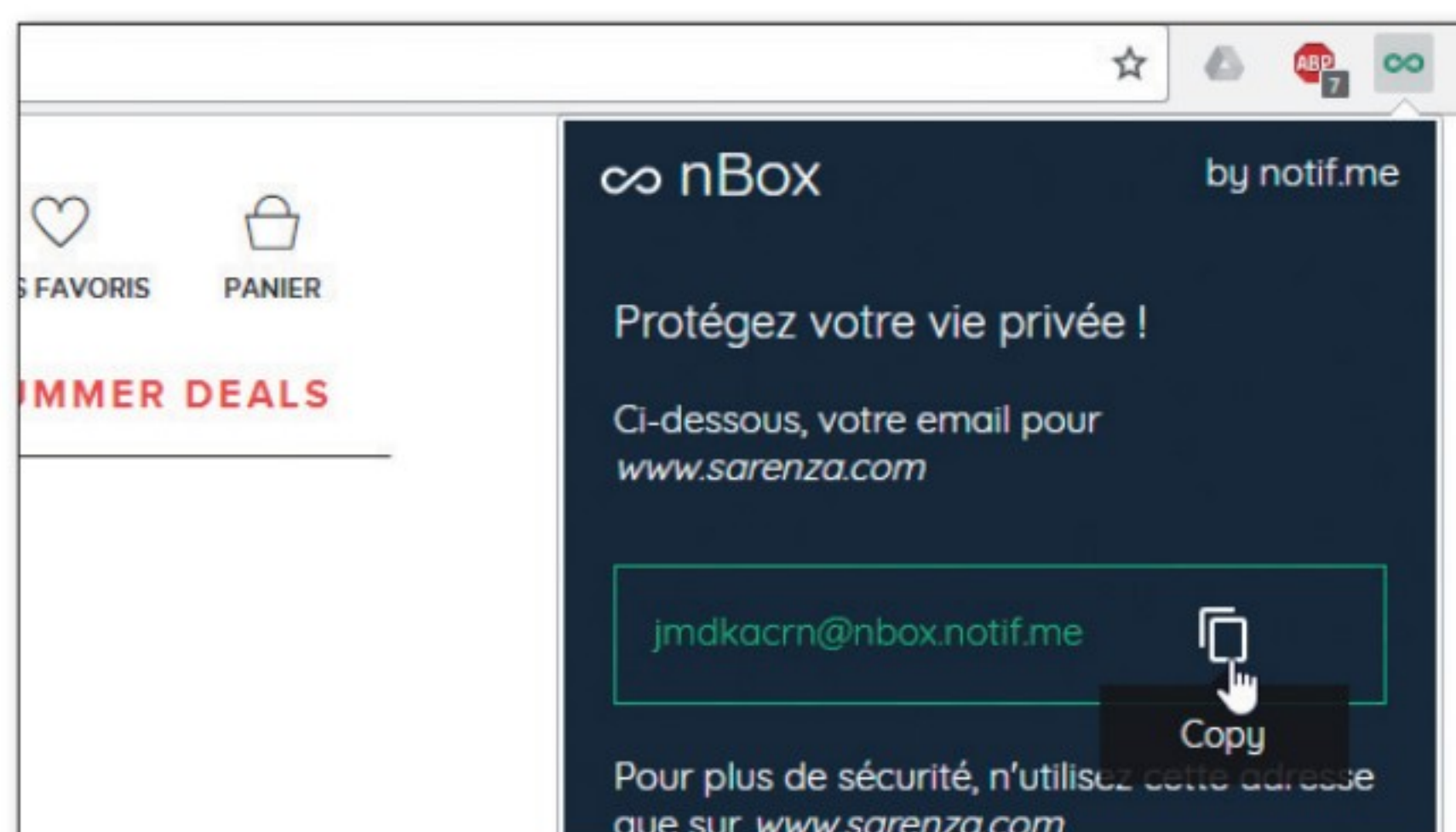
Vous n'avez pas envie de donner votre adresse mail pour vous inscrire à tel ou tel service ? L'extension Chrome nBox crée des adresses anonymes.



INFOS [nBox pour chrome]

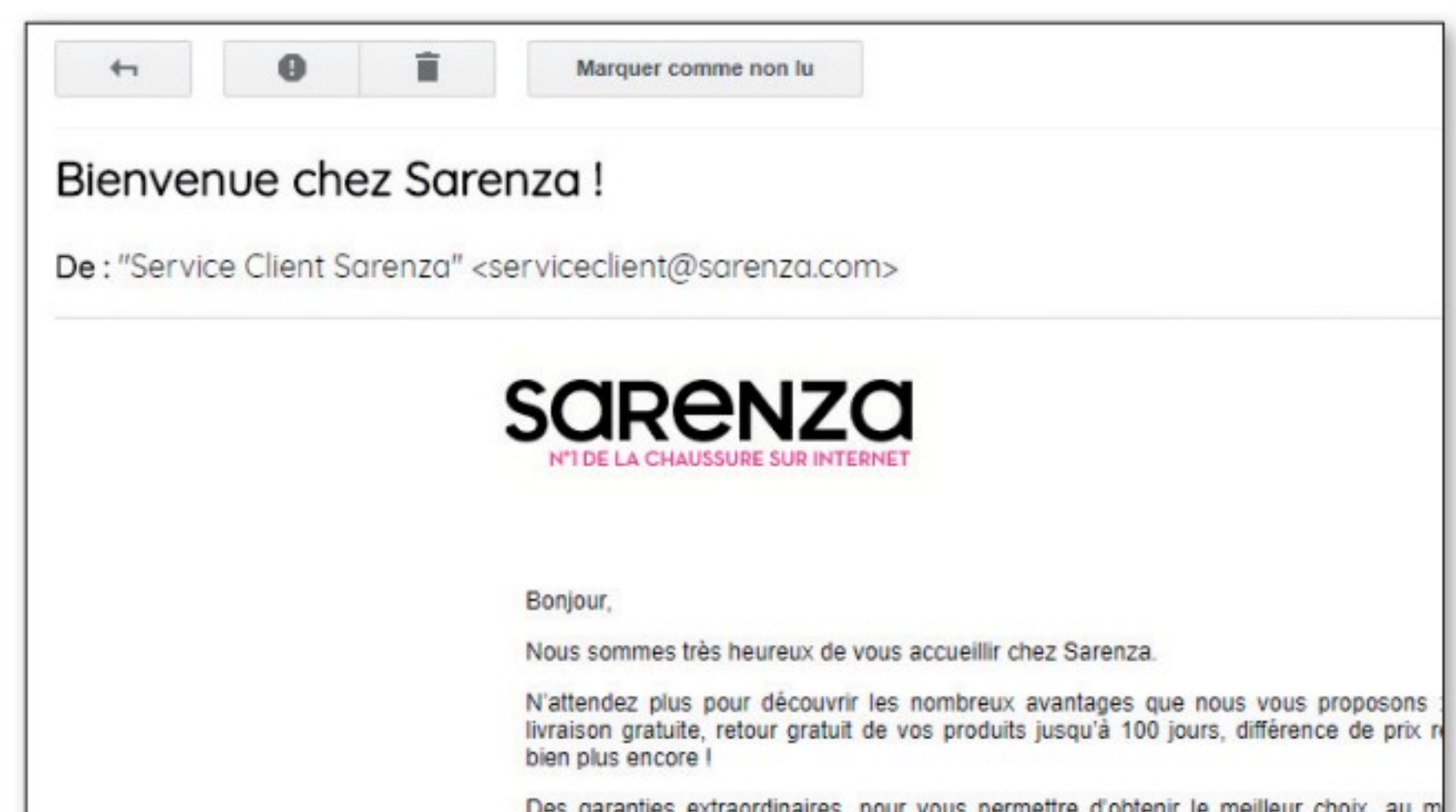
Où le trouver ? [<https://goo.gl/fqF6ZK>]

Difficulté :



01 > CRÉER UNE BOÎTE MAIL

Après l'installation de l'extension, allez sur le site qui vous demande une adresse mail. Cliquez sur l'icône de nBox, **Générer une adresse** puis le symbole de la copie. Collez l'adresse dans le formulaire et terminez l'inscription au service normalement.



02 > CONSULTER LES MESSAGES

Cliquez sur le logo de nBox puis sur **Mon nBox**. Sélectionnez un mail pour le lire ou le supprimer. Notez que toutes les adresses que vous avez créées via nBox partagent la même boîte de réception.



DECRYPTAGE

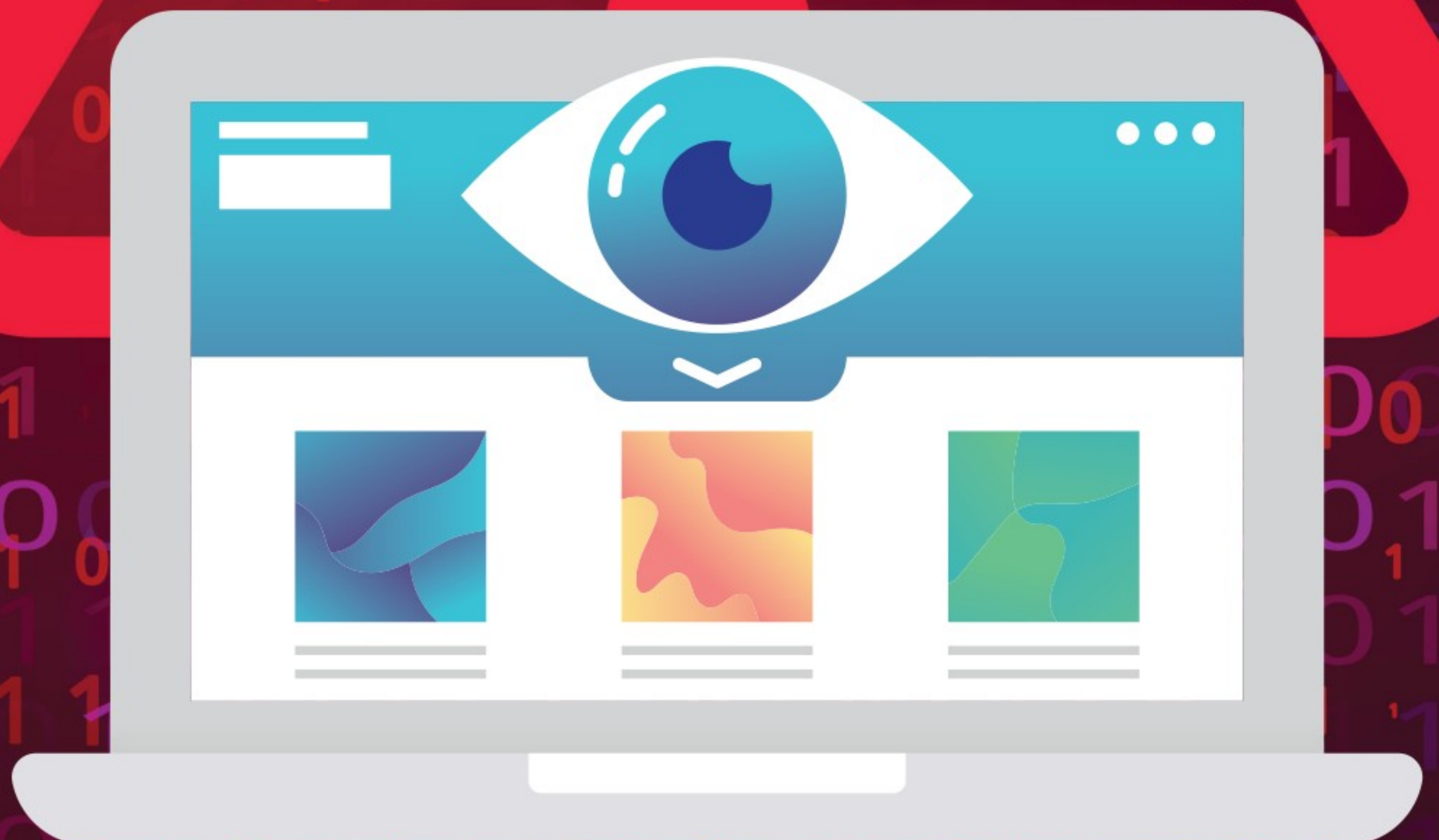
ATTENTION AUX LOGICIELS ESPIONS POUR PC

TEST DE HOVERWATCH

Mais que fait la police ?

Ils sont désormais accessibles au plus grand nombre et peuvent être utilisés par des personnes sans connaissances informatiques. Ils ont pignon sur Web, même pas besoin de passer par le darknet. Payants, ces services clés en main s'installent facilement sur votre PC et se font extrêmement discrets.

Dans notre dernier numéro, nous vous mettons en garde contre MSpy, une appli espion puissante qui s'installe sur téléphone portable. Elle est présentée comme un outil destiné à surveiller l'activité des enfants, mais personne n'est dupe : la société derrière MSpy, qui serait ukrainienne, mais domiciliée dans un paradis fiscal, vise le marché grand public de l'espionnage domestique ou en petites entreprises.





HACKING

Dans le même état d'esprit, nous avons découvert Hoverwatch. Moins puissant que mSpy, il cible bien sûr la surveillance sur mobile. Mais nous avons aussi remarqué qu'il disposait d'une version Windows (et même Mac), c'est celle que nous avons étudiée ici pour connaître le détail de ses fonctionnalités. Bien sûr, rien n'est gratuit, sauf les quelques jours d'essai : il s'agit d'un logiciel payant, sur abonnement (à partir de 24,95 € pour 1 mois et 1 seul appareil !). Un business qui franchit clairement les limites de la légalité, mais qui semble faire florès depuis quelques années déjà sans que le législateur impose sa fermeture.

Pour rappel, espionner des personnes sans leur consentement est illégal. En France, l'article 226-1 du Code pénal punit de 45 000 euros d'amende et d'un an de prison ferme l'atteinte à la vie privée d'autrui. De quoi calmer quelques ardeurs...

RÉUNIR SOUS UN SEUL LOGICIEL PLUSIEURS TYPES DE SPYWARES

Ces keyloggers améliorés (ils se présentent sous cette appellation, même si leur champ d'action est plus large) permettent non seulement de savoir tout ce qu'une personne tape sur son clavier, mais aussi de réaliser des captures de son écran à son insu ou de lister toutes ses actions. Certains d'entre eux ont même accès à la webcam, aux micros, voire aux périphériques (comme les imprimantes. Il est loin le temps où il était possible d'utiliser le matériel de l'entreprise à son propre profit...). Si une personne se connecte sur un réseau social plutôt



que d'utiliser uniquement son logiciel de travail, c'est indiqué. De même que l'adresse des sites internet sur lesquels elle se rend. Chaque action fait l'objet d'un enregistrement dédié. Plus rien, ou presque, n'est privé !

EN DIRECT OU EN DÉCALÉ

Sur PC, Hoverwatch permet de vérifier rapidement ce que fait, ou ce qu'a fait, un utilisateur. Il est en effet possible d'accéder à un aperçu en direct de l'écran de la personne surveillée tout comme de consulter un journal des activités et de tout ce qui a été écrit, en fin de journée ou de semaine. Il surveille même le contenu de vos échanges Skype. Avec des filtres divers, le client pourra se concentrer uniquement sur ce qui l'intéresse ou sur qu'il a envie de savoir.

The screenshot shows the Hoverwatch website with three pricing plans:

- Personal:** from €24.95 per month, Track 1 Device. All monitoring functions are available. Options: €24.95 (1 month), €59.95 (3 months), €99.95 (12 months).
- Professional:** from €9.99 per month / device, Track 5 Devices. All monitoring functions are available. Mobile Viewer. Options: €49.95 (1 month), €99.95 (3 months), €199.95 (12 months).
- Business:** from €6.00 per month / device, Track 25 Devices. All monitoring functions are available. Mobile Viewer. Options: €149.95 (1 month), €299.95 (3 months), €499.95 (12 months).

At the bottom, it states: "Compatibility: Android / Windows PC / Mac Computer" and "Secure online payment: VISA, MasterCard, American Express, PayPal, JCB, Alipay".

DES PRIX PROHIBITIFS POUR DES FONCTIONS FINALEMENT ASSEZ BASIQUES. MAIS CE QUI EST VENDU À L'UTILISATEUR, C'EST LA RÉUNION DE CES DERNIÈRES SOUS UNE SEULE INTERFACE ET UNE ERGONOMIE ACCESSIBLE AUX DÉBUTANTS.





QUE PERMET VRAIMENT HOVERWATCH ?

PRATIQUE



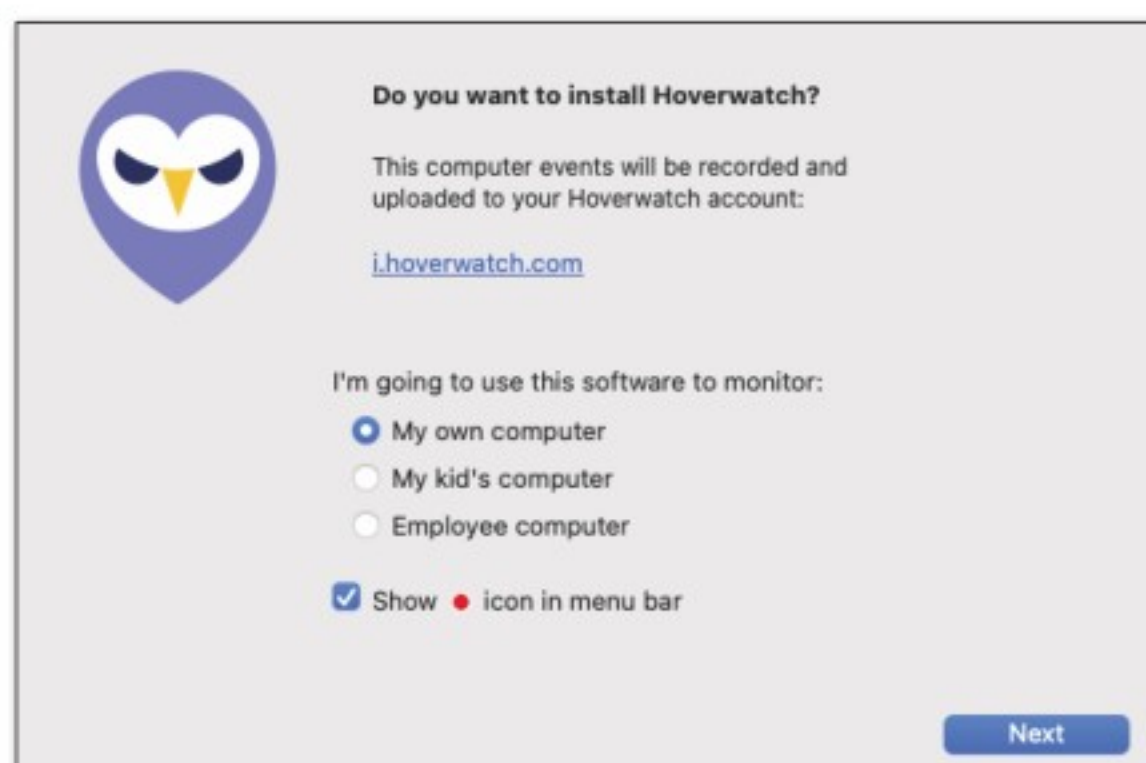
01 > INSTALLER LE LOGICIEL

Depuis notre navigateur, nous créons notre compte. L'identifiant et le mot de passe sélectionnés seront utiles pour configurer le logiciel une fois qu'il sera téléchargé. Un mot de passe, indiqué sur la page de téléchargement, sera aussi à rentrer. Le cas échéant, il est nécessaire de désactiver son antivirus ou d'autoriser l'installation.



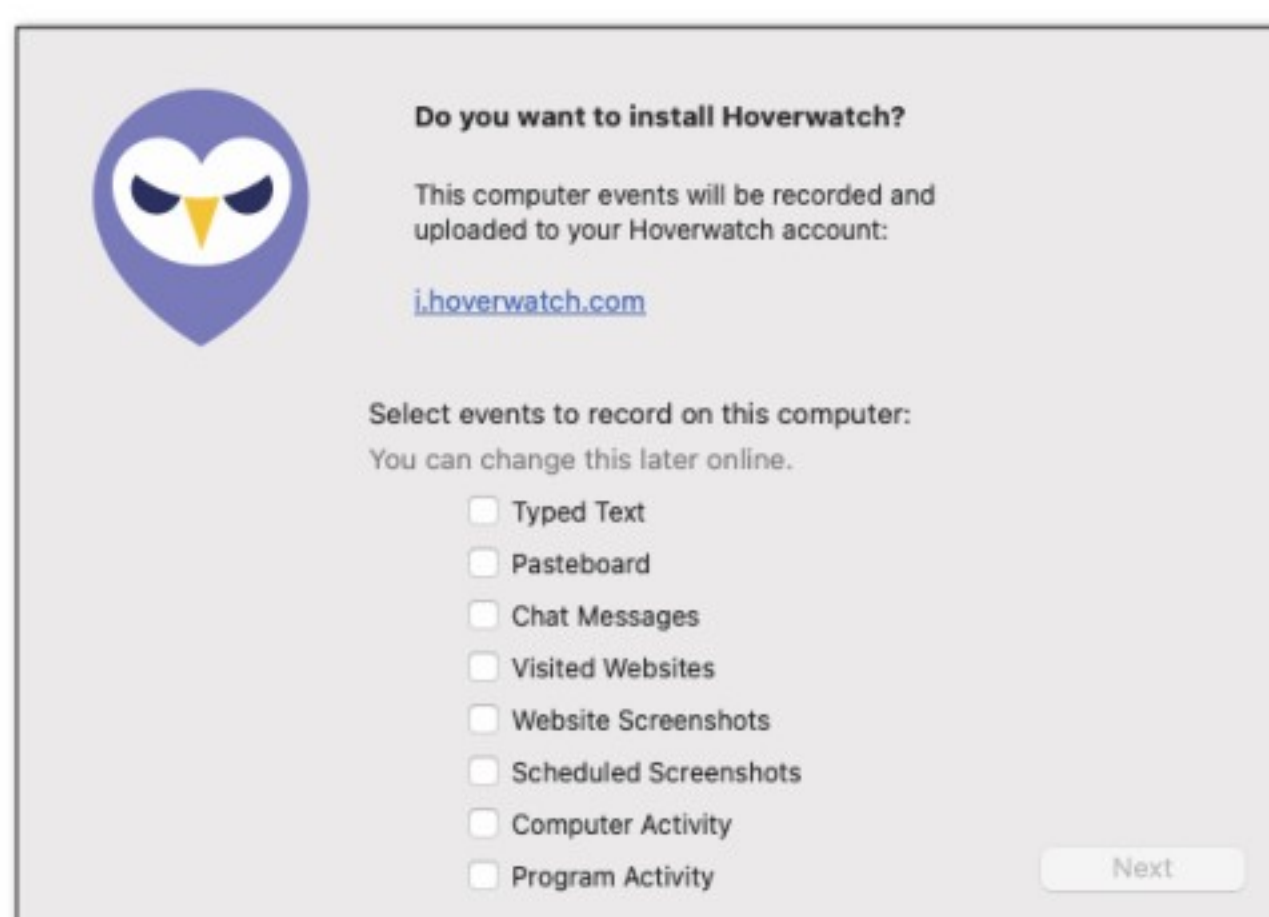
02 > CHOISIR COMMENT SURVEILLER

Il nous a d'abord été demandé pour quel type d'ordinateur nous voulions installer Hoverwatch. Vous pouvez surveiller vos enfants, vos employés... ou vous-même (!). Ici, nous pouvons décocher l'apparition de l'icône de surveillance afin que celle-ci reste indétectable.



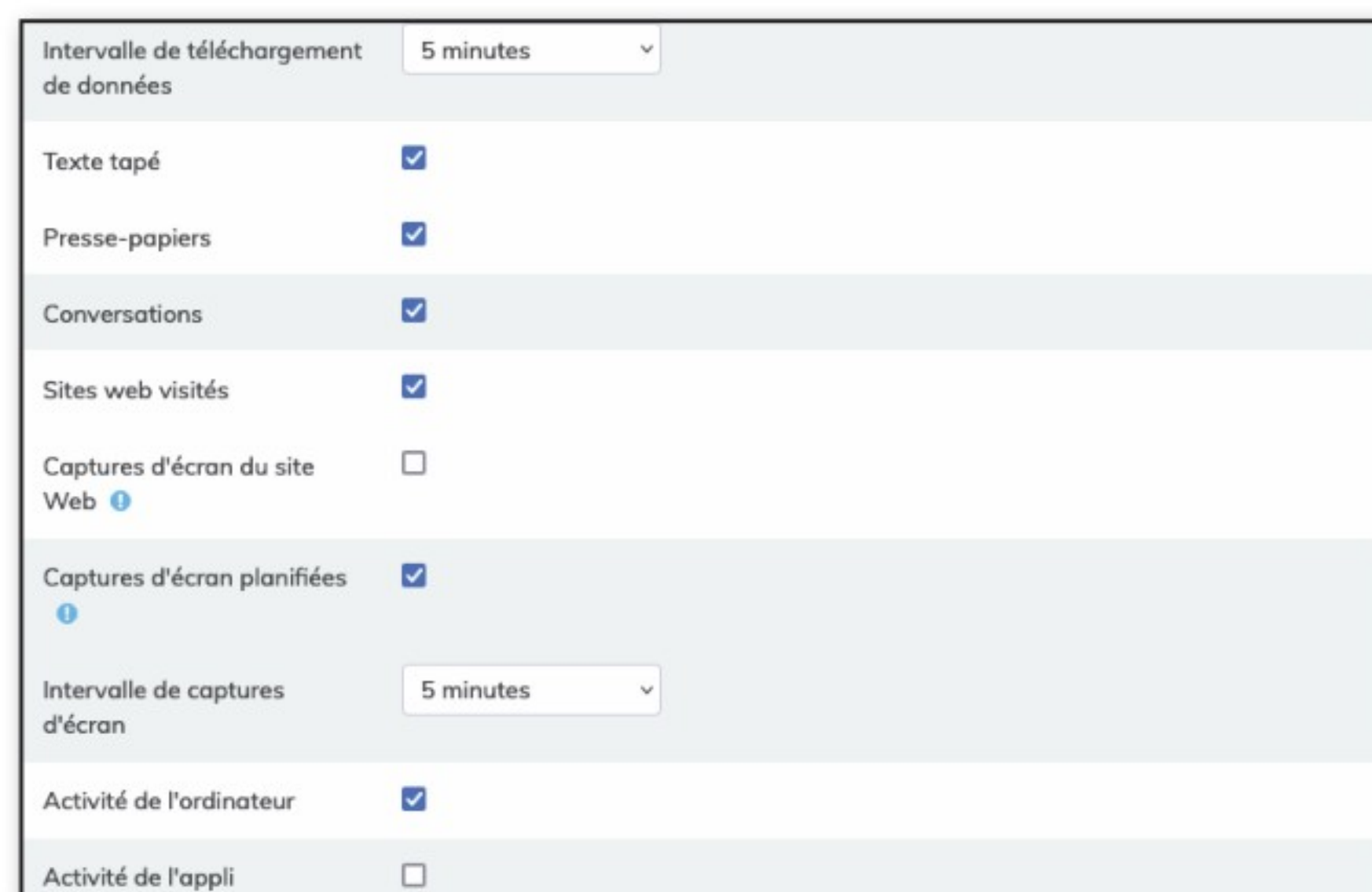
03 > SÉLECTIONNER LES ÉVÉNEMENTS À ENREGISTRER

Hoverwatch permet de superviser de nombreuses activités. Il n'a pas accès à la webcam ou au micro, mais par contre, vous pouvez décider d'enregistrer des captures d'écran régulières, les messages tapés au clavier, les sites visités... Il nous a suffi de sélectionner et de cocher ce qui nous intéressait (choix modifiable par la suite).



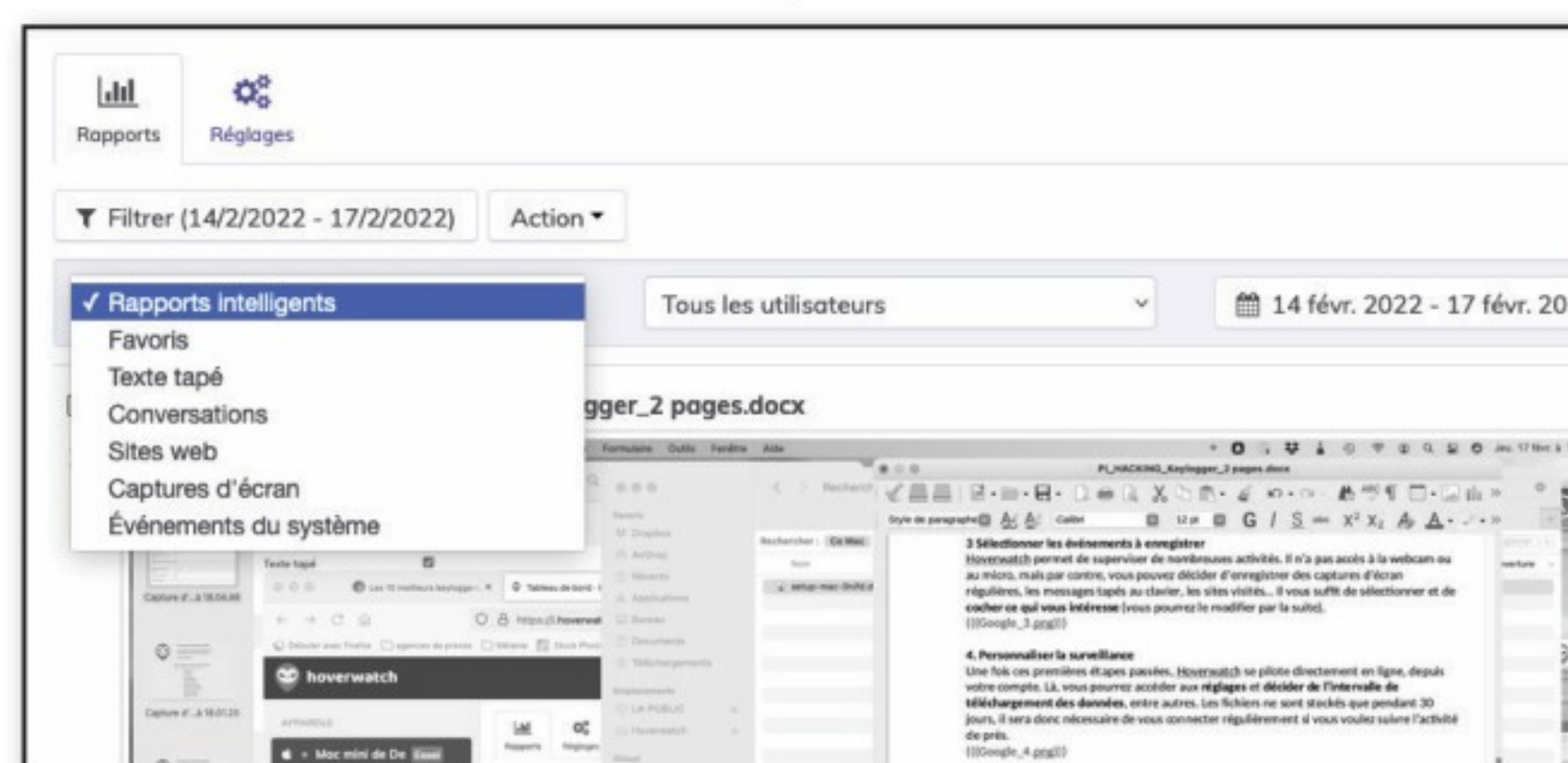
04 > PERSONNALISER LA SURVEILLANCE

Une fois ces premières étapes passées, Hoverwatch se pilote directement en ligne, depuis notre compte. Là, nous pouvons accéder aux réglages et décider de l'intervalle de téléchargement des données, entre autres. Les fichiers ne sont stockés que pendant 30 jours, il sera donc nécessaire de se connecter régulièrement si pour suivre l'activité de près.



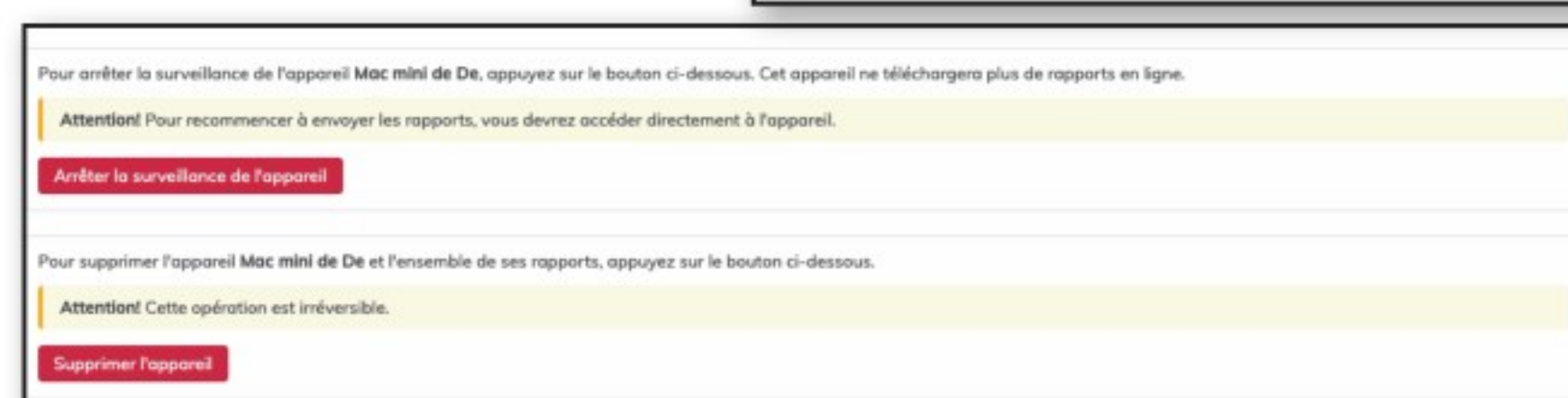
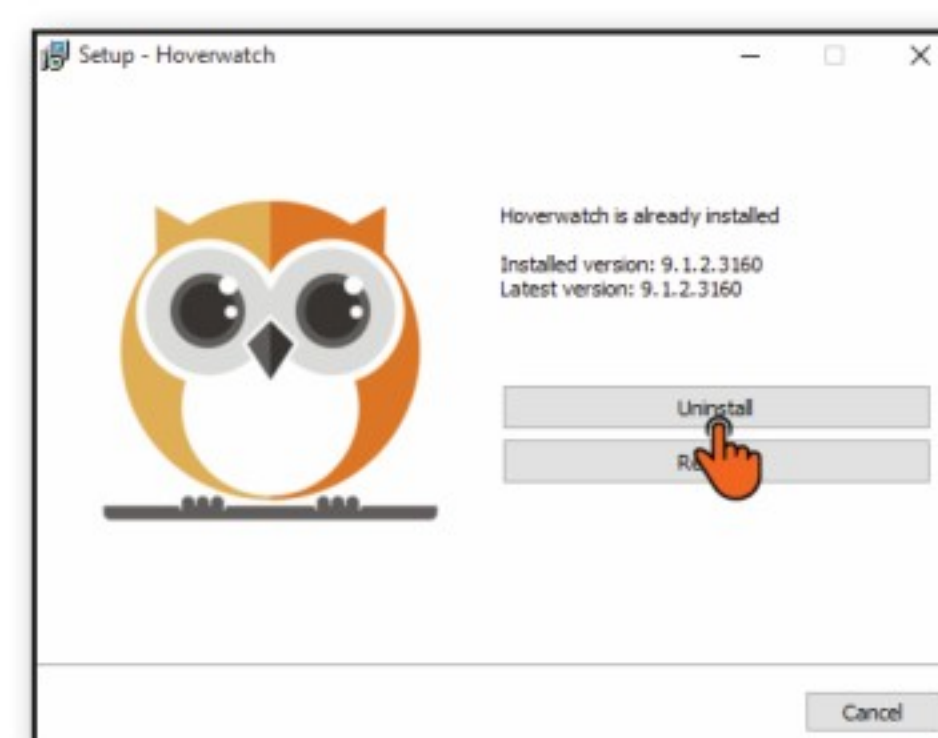
05 > ACCÉDER AUX RAPPORTS

Depuis ce même compte, nous avons accès aux rapports d'activité. Selon les besoins, nous pouvons utiliser des filtres, afin d'afficher uniquement certains éléments.



06 > ARRÊTER LA SURVEILLANCE

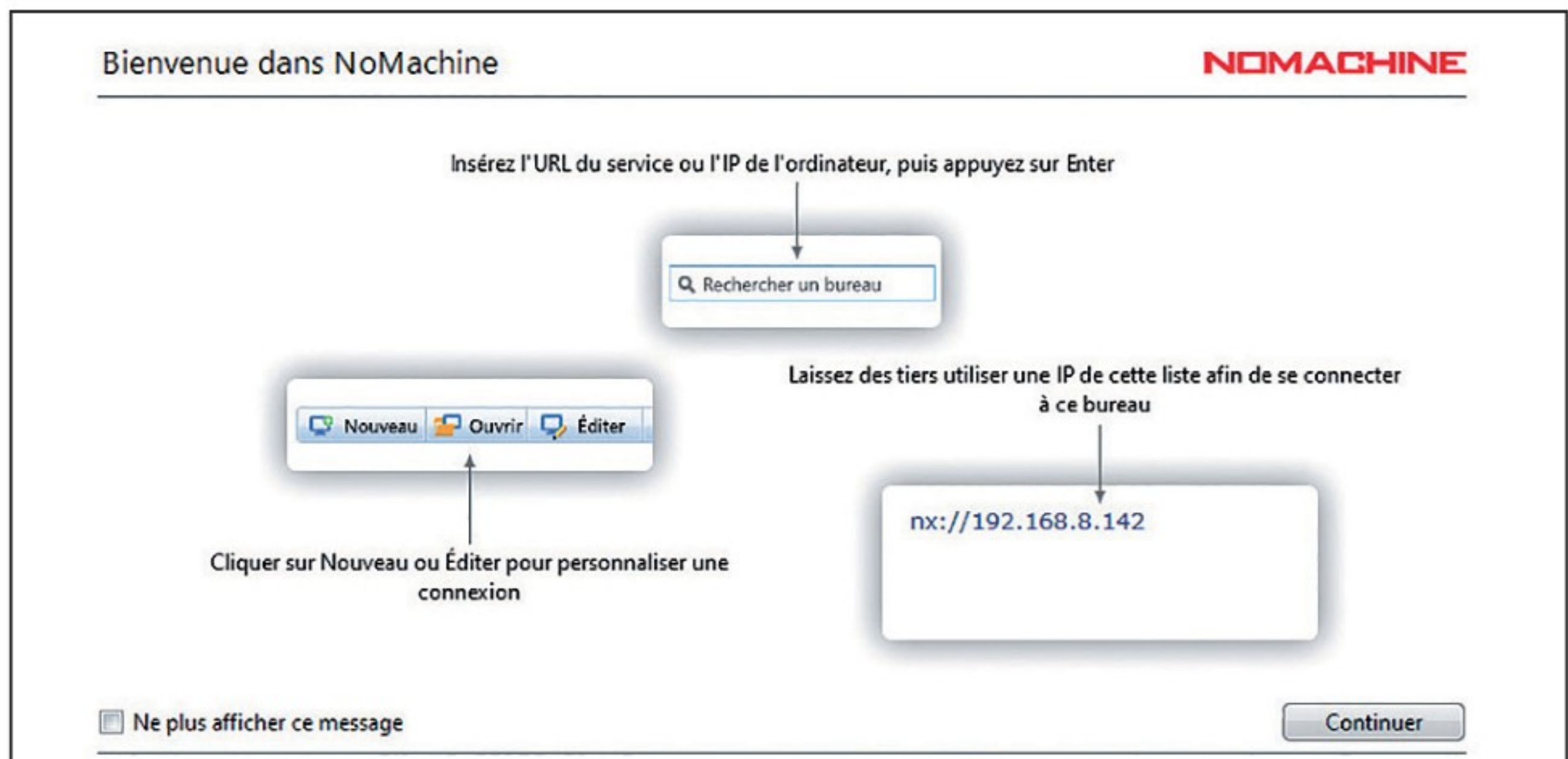
Si vous voulez en supprimer un pour en ajouter un autre, allez dans **Réglages** et cliquez sur **Arrêtez la surveillance de l'appareil**. Vous pouvez aussi décider de supprimer le logiciel de l'appareil.





Prise de contrôle à distance > AVEC NoMACHINE

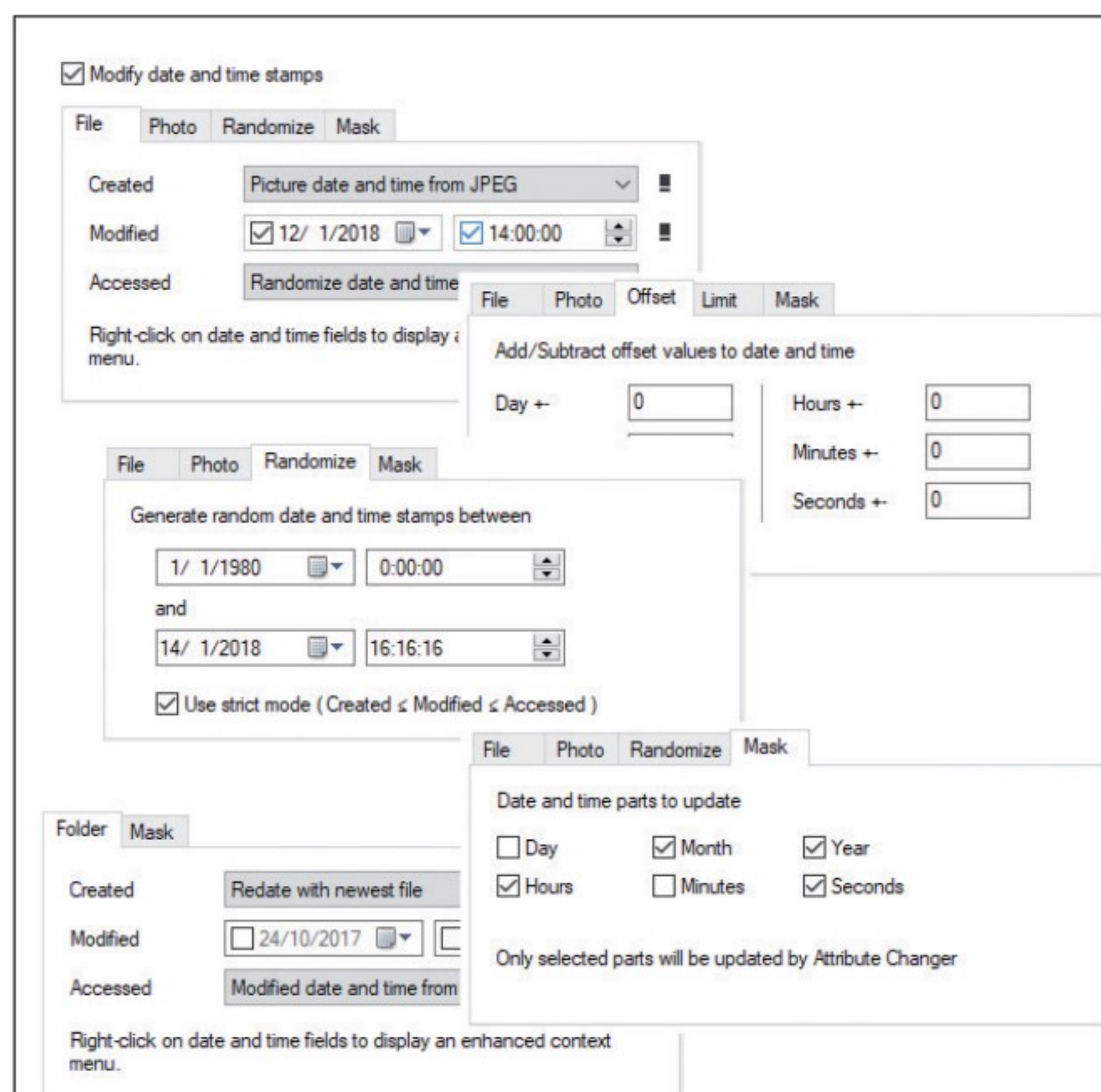
Pas vraiment connu, NoMachine est pourtant une excellente solution de contrôle à distance. Gratuit et multi-plateforme, il permet de se connecter grâce à un identifiant, et de gérer plusieurs ordinateurs. Le top ? La fluidité garantie par le protocole NX, et la sécurité assurée grâce au SSH. L'utilisateur est guidé étape par étape, et peut configurer NoMachine en finesse. Un logiciel à découvrir !
Lien : <http://keit.co/p/recall>



Changer les attributs d'un fichier ou dossier > AVEC ATTRIBUTE CHANGER

Attribute Changer vous donne la main sur les attributs d'un fichier ou d'un dossier (date et heure de création ou modification, lecture seule, système, caché, archive et indexé, etc.). Il vous permet de les modifier et donc de leur donner une nouvelle identité pour, par exemple, masquer ses origines. Une fois Attribute Changer installé, ce programme gratuit sera accessible via le clic droit de votre souris sur le fichier ou dossier cible. Vous avez la possibilité de modifier les attributs de fichiers un par un ou par lot. Un mode Simulation vous permet de vérifier le résultat avant toute modification.

Lien : www.petges.lu

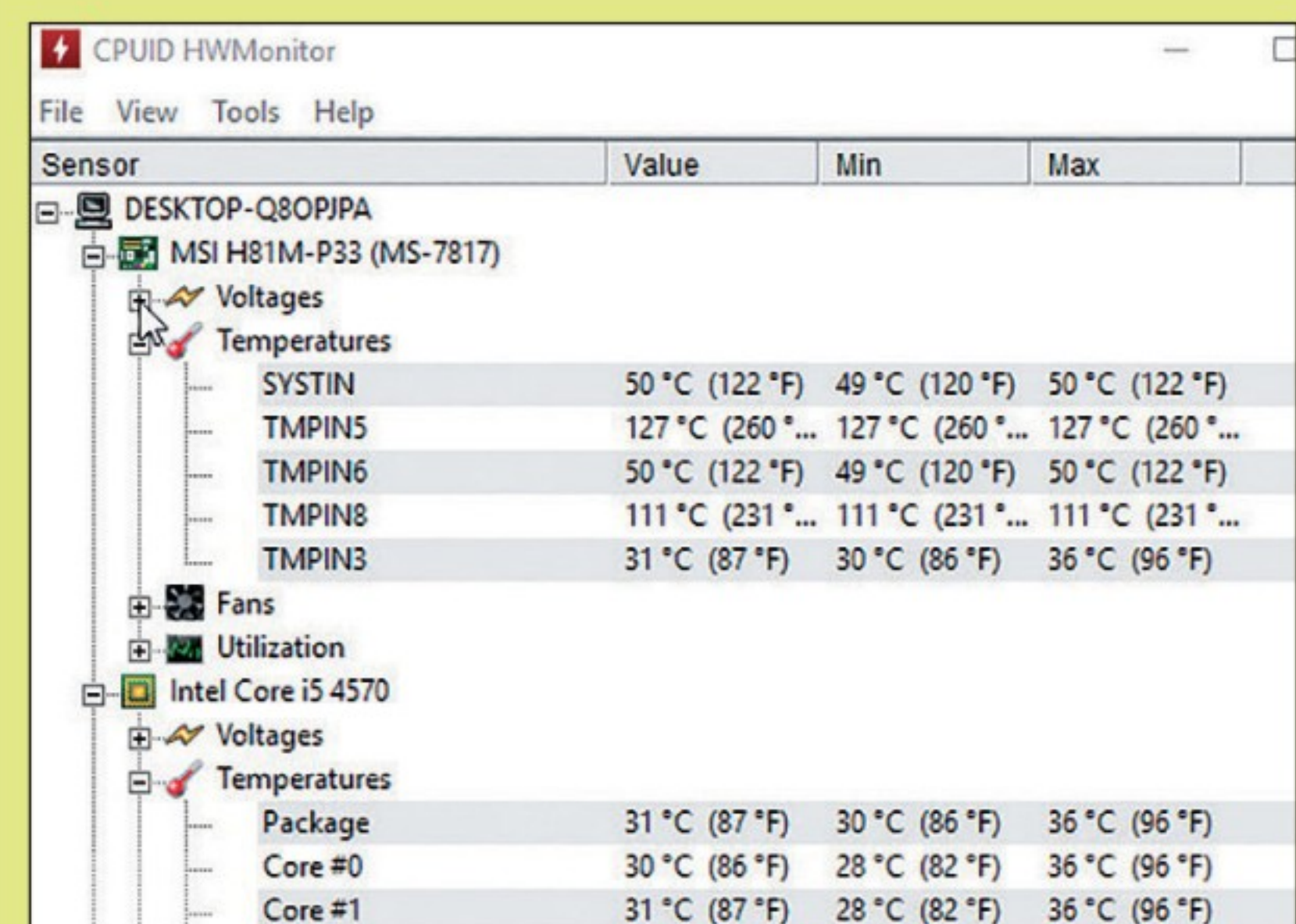


Prenez la température de votre PC > AVEC HWMONITOR

Surveiller la température de votre PC permet d'éviter une surchauffe, qui peut nuire à vos composants et provoquer des dysfonctionnements. Dès le lancement de HWMonitor, toutes les données s'affichent.

Pour y voir plus clair, n'hésitez pas à réduire tous les paramètres autres que **Temperatures** en cliquant sur le petit - en début de ligne. Vous retrouvez un onglet **Temperatures** pour chaque composant : la carte-mère, le CPU, les disques durs et la carte graphique.

Lien : <https://tinyurl.com/hwmonitorTA>



Comme dans une série américaine, le papier peut revenir pendant plusieurs saisons.

La force de tous les papiers, c'est de pouvoir être recyclés
au moins cinq fois en papier. Cela dépend de chacun de nous.
www.recyclons-les-papiers.fr

Tous les papiers ont droit à plusieurs vies.
Trions mieux, pour recycler plus !

Votre publication s'engage pour
le recyclage des papiers avec Ecofolio.





TOP 7

ALTERNATIVES POUR TOUT FAIRE SANS GOOGLE

Plus envie de sacrifier votre âme numérique au côté pratique et (ultra-performant) de Google ? Savez-vous que des alternatives à ses principaux services existent et vous offriront des fonctionnalités et outils qui concurrencent la toute puissance du géant américain ? Le tout sans aspirer vos données personnelles et gratuitement ! Une sélection rigoureuse pour se désintoxiquer de la galaxie Google.

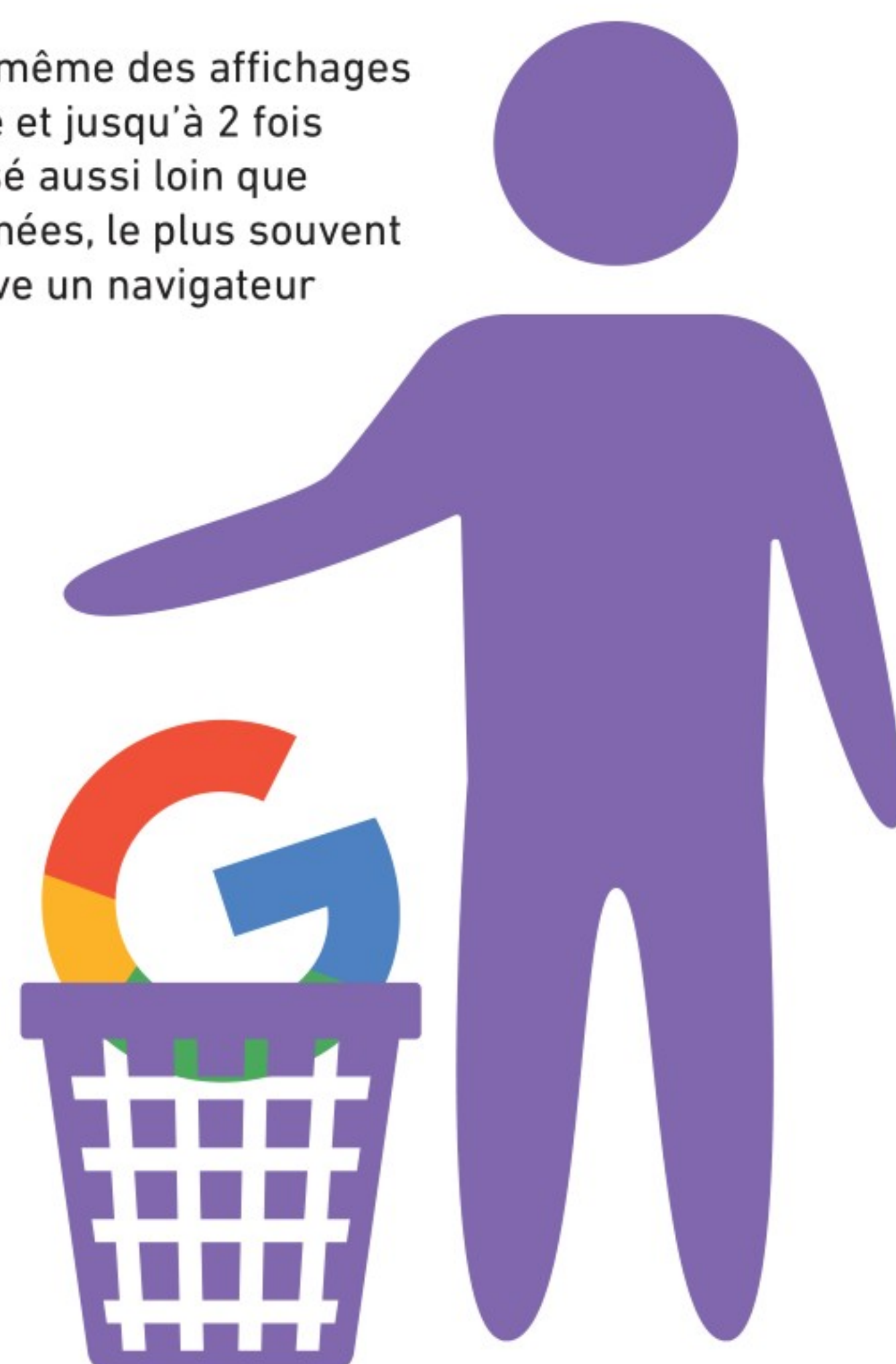
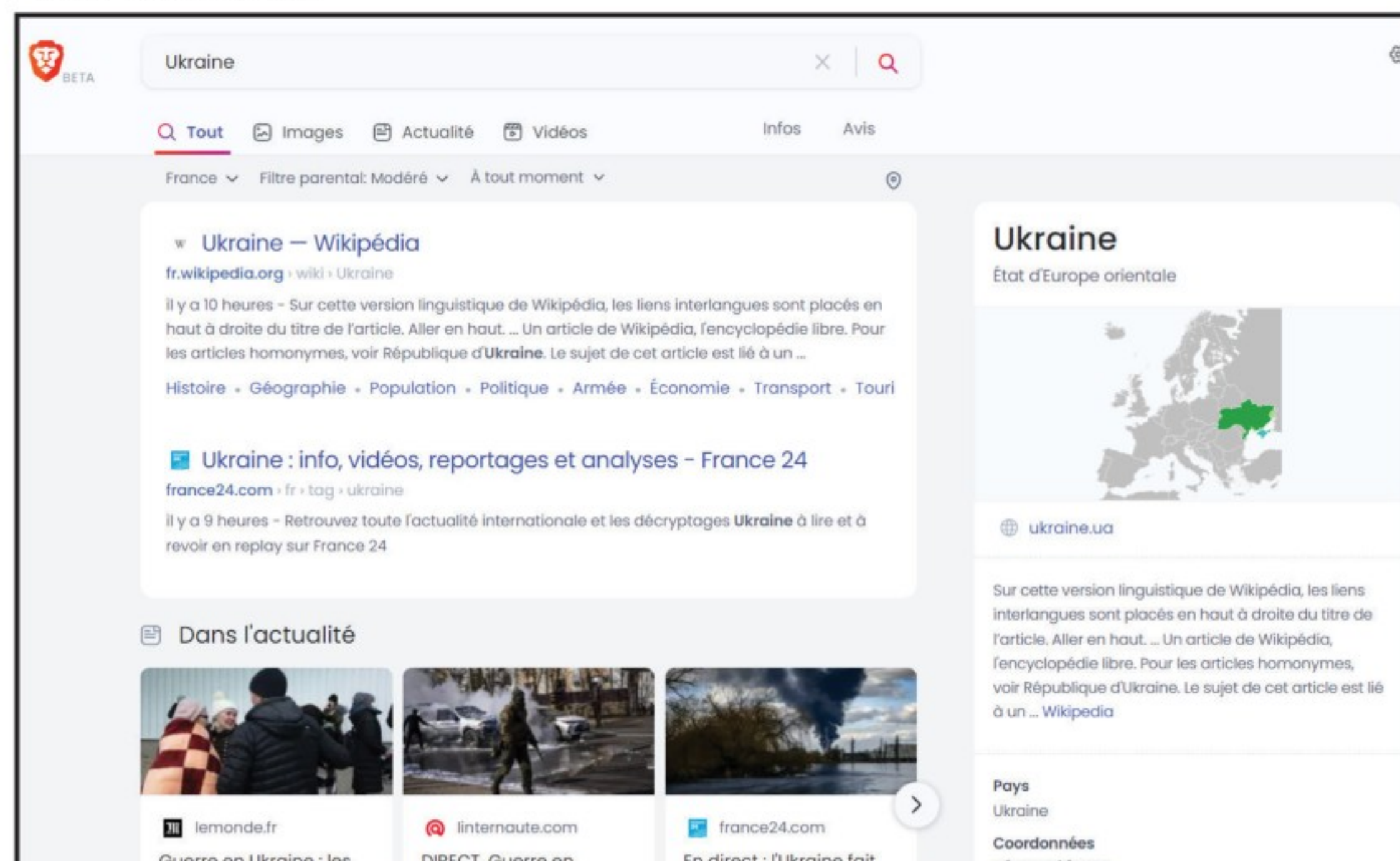
CHROME

> Passez à Brave



Un petit gars tout ce qu'il y a de sympathique... qui annonce quand même des affichages de pages jusqu'à 8 fois plus rapides que Google Chrome sur mobile et jusqu'à 2 fois plus rapides sur PC. La raison ? Basé sur Chromium, Brave a poussé aussi loin que possible la suppression de toutes les collectes et injections de données, le plus souvent synonymes de traçage et d'espionnage marketing. Du coup, l'utilisateur retrouve un navigateur sécurisé et allégé, sans perdre ses habitudes de navigation.

Lien : brave.com



GMAIL

> Passez à TUTANOTA



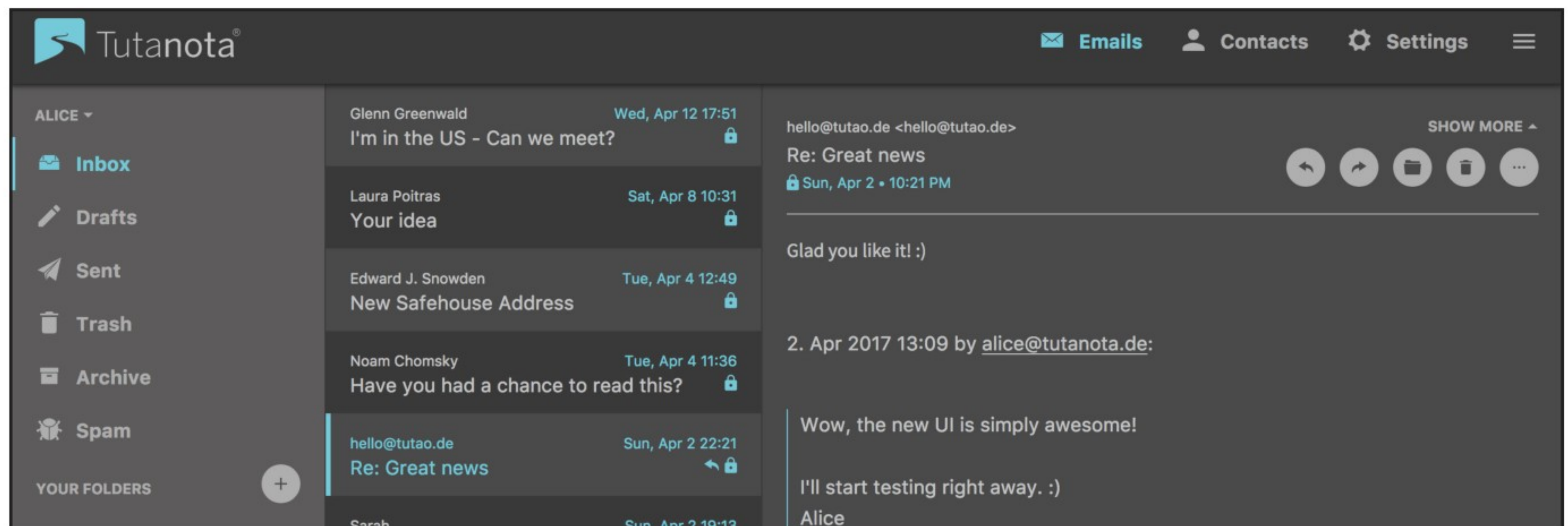
Le mot Tutanota est dérivé du Latin et contient les mots «tuta» (sécurisé) et «nota» (message, note). Voici pour l'étymologie de cette messagerie gratuite et open source développée à Hanovre, en Allemagne. Tutanota est gratuite dans sa version « 1 Go de stockage » pour les particuliers. Avec le chiffrement de bout-en-bout et l'A2F, personne (y compris Tutanota) ne peut déchiffrer ou lire vos données. Des version mobiles Android et iOS sont bien sûr disponibles. Un nom de domaine ainsi qu'un calendrier sont proposés en sus dans cette version gratuite.

Lien : tutanota.com

GMAIL, VOTRE MEILLEUR ENNEMI



Gmail est le coeur de la stratégie Google, tous ses services passent par la création d'un compte idoine. C'est la porte d'entrée marketing la plus puissante du géant américain puisque tous vos messages et connexions sont scannés et les datas ainsi collectées alimentent ses outils à des fins pratiques mais aussi publicitaires. Et depuis que Google permet aux éditeurs de solutions tierces d'utiliser vos logins Gmail comme moyen d'identification, ces mêmes sociétés sont autorisées à accéder à une partie de vos données privées et de les mouliner dans leurs système d'apprentissage automatique.



DRIVE

> Passez à TRESORIT

Encrypté de bout en bout, 3 Gb offerts dans sa version gratuite et 500 Mo par fichier pour les transferts. Par contre, pas de gestion collaborative, le service est principalement destiné à l'échange sécurisé de gros fichiers.

Lien : send.tresorit.com



Learn more

Add your files
Up to 5 GB

By clicking 'Create Secure Link' you agree to the [Terms of Service](#) and [Privacy & Cookie Notice](#).

Create Secure Link

The most secure file sending solution in the known universe

End-to-End Encrypted

SWISS Privacy

GDPR Compliant Technology



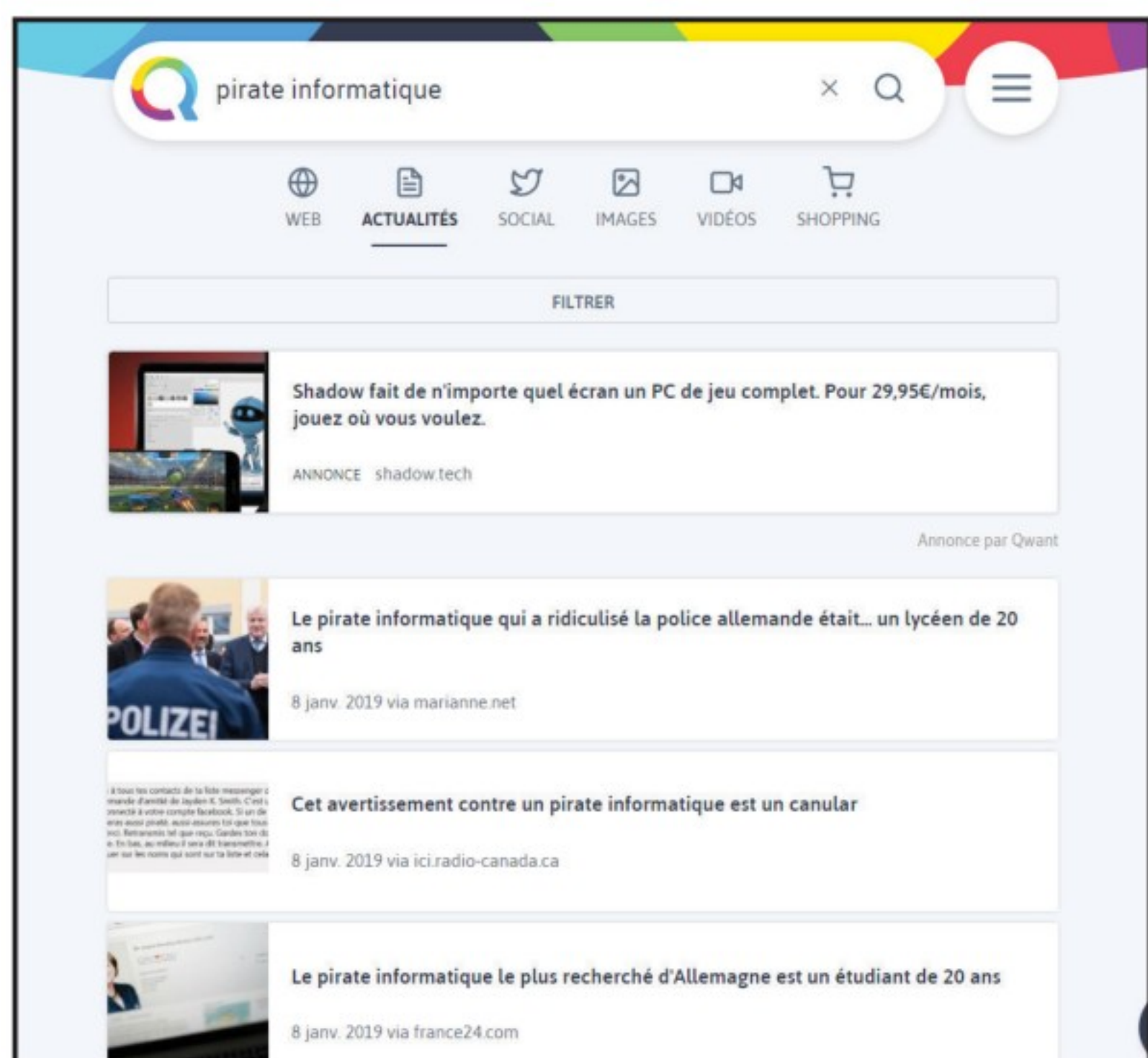
ANONYMAT

MOTEUR DE RECHERCHE

> Passez à QWANT



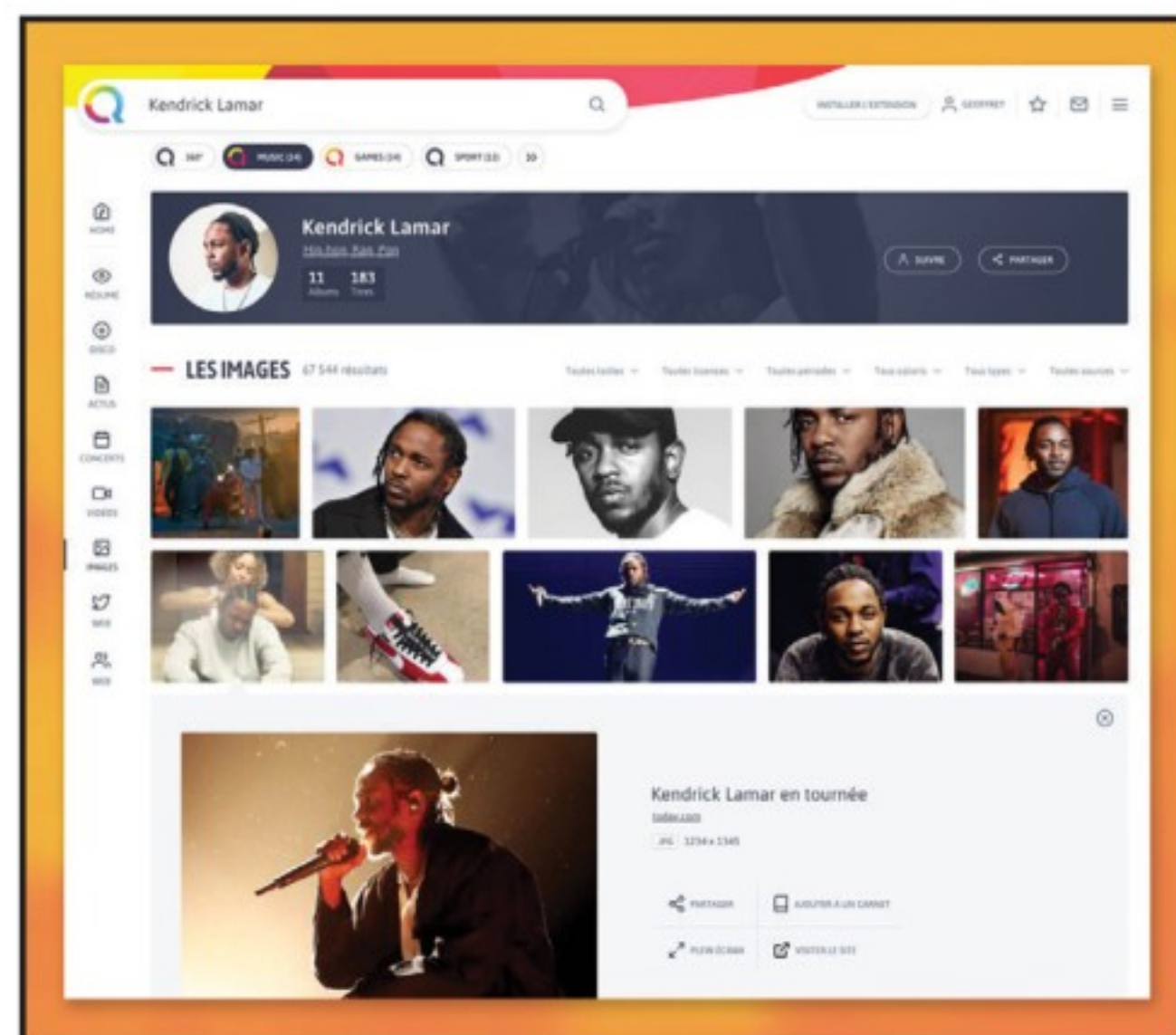
Vous le savez, Qwant est depuis quelques années le chouchou de la rédaction. Peut-être y-a-t-il ici quelque chauvinisme puisque Qwant est un moteur de recherche franco-européen. Mais c'est surtout l'esprit, l'ambition technique affichée et la qualité finale du search engine qui nous séduisent et en font un concurrent crédible à Google pour tous les amoureux de la protection des données.



NEUTRALITÉ DES RECHERCHES

Preuve de sa maturité, Qwant est devenu le moteur de recherche par défaut du Ministère français des armées. Qwant n'installe pas de cookies traceurs et ne piste pas ses utilisateurs, le seul cookie présent n'existe que durant la session et est supprimé immédiatement après. Les résultats affichés sont neutres et ne sont pas personnalisés d'après un historique de recherche comme pour Google, Qwant n'en possédant pas, mais dépendent uniquement des tendances du moment, en partie d'après les réseaux sociaux. Qwant ambitionne de devenir un véritable écosystème de services (comme Google) avec un module de paiement sécurisé intégré mais aussi d'autres outils grand public comme Qwant Junior ou le très bon Qwant Maps.

Lien : www.qwant.com



MAPS

> Passez à OPENSTREETMAP



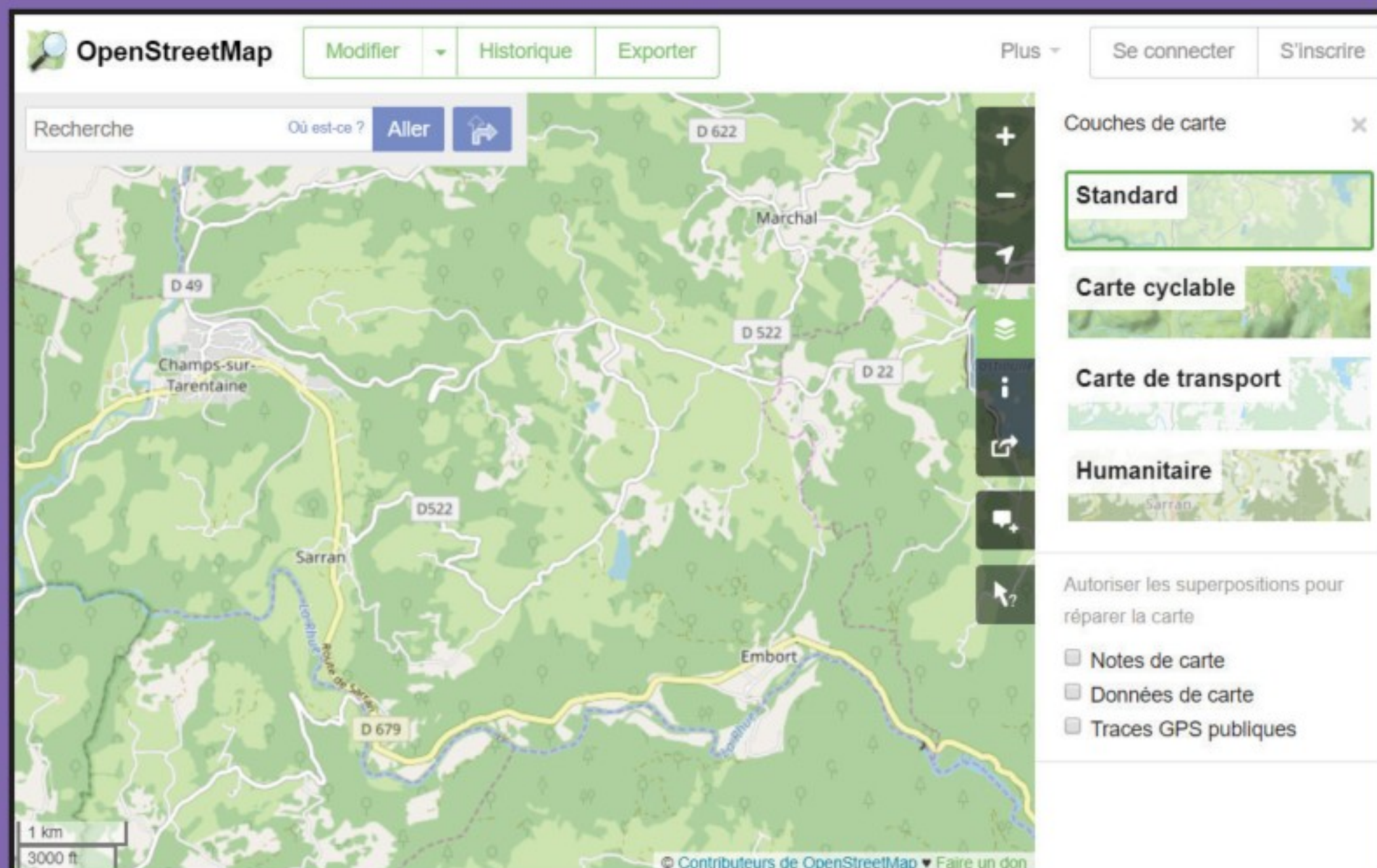
OpenStreetMap est un service de cartographie gratuit et open source, ce qui signifie que de nombreux développeurs se le sont approprié pour proposer leur propre outil personnalisé, pour plusieurs plateformes

(PC, Mac, Android, iOS notamment) et en ajoutant des fonctionnalités bienvenues. La base OpenStreetMap a cependant été conçue pour un environnement Windows/PC. Mais vous trouverez des variantes mobile comme l'application **OsmAnd** (Android et iOS).

PAS DE COMPTE, PAS DE PUB

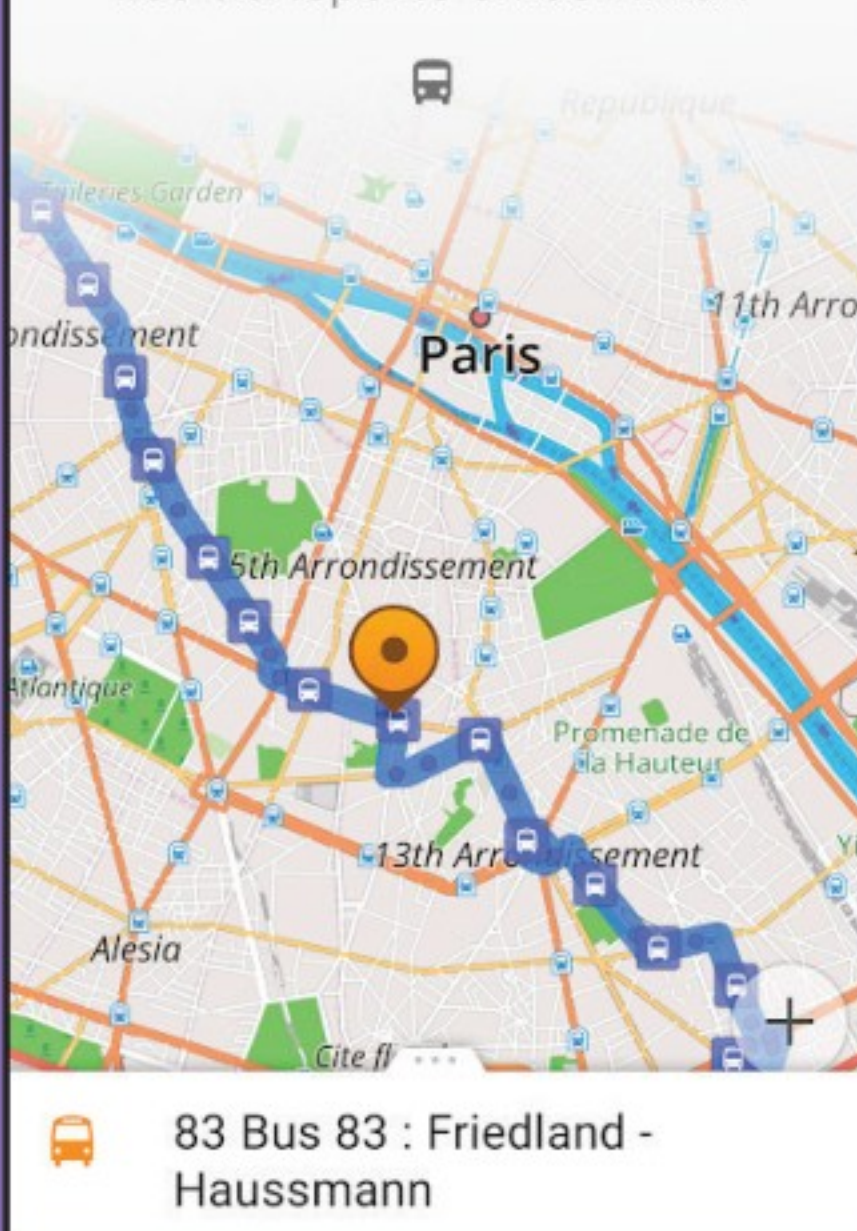
Le gros plus de OpenStreetMap et de ses déclinaisons, contrairement à Google Maps, c'est de pouvoir utiliser le services sans compte associé, c'est à dire en évitant le tracking centralisé même si la localisation GPS est bien sûr un impondérable la plupart du temps. La désactivation du GPS est cependant très simple et vos informations de localisations peuvent être maintenues complètement privées.

Lien : www.openstreetmap.org



TRANSPORT PUBLIC

Métro, tramway et bus,
Les transports en commun



YOUTUBE

> Passez à YOUTUBE VANCED

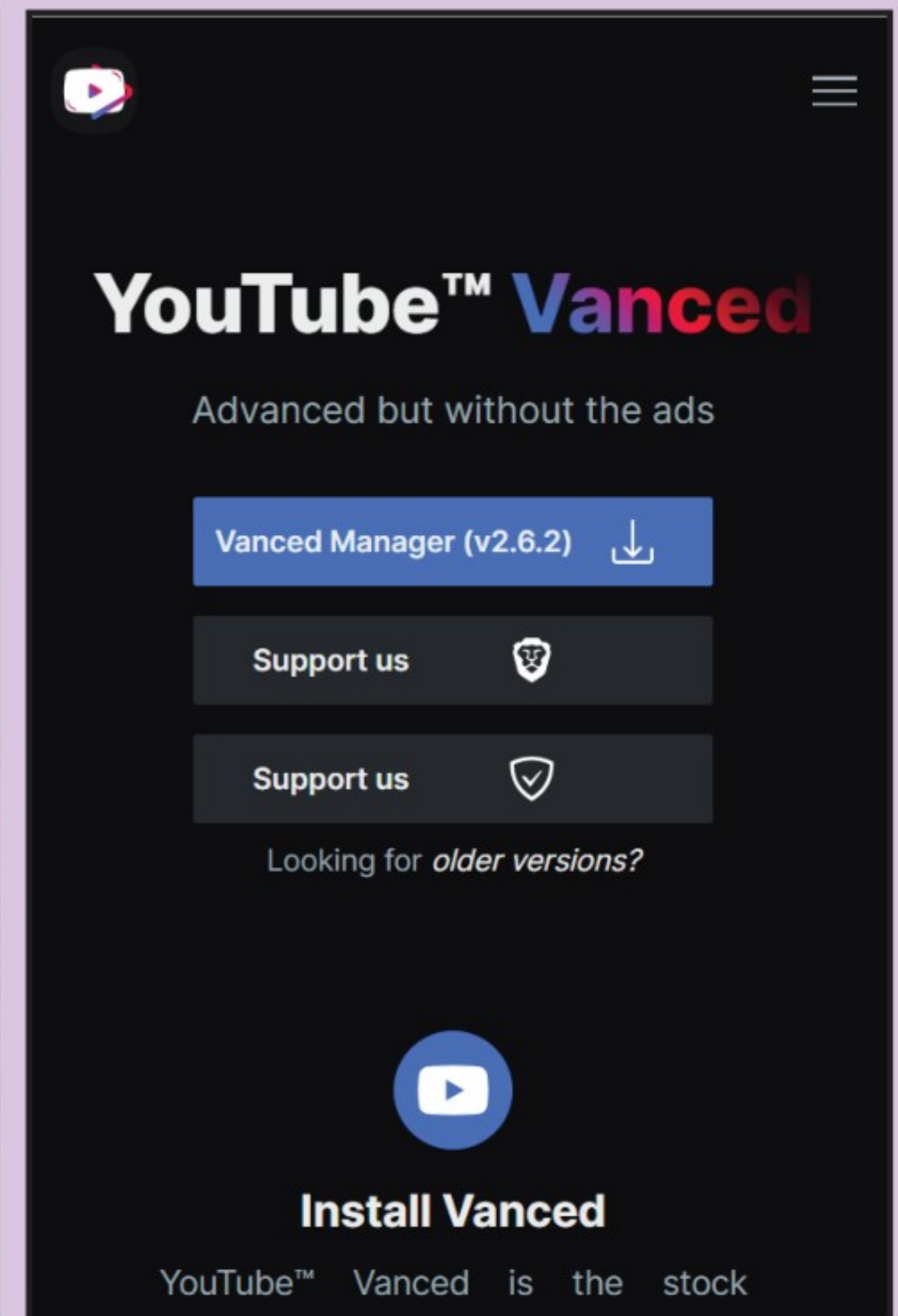
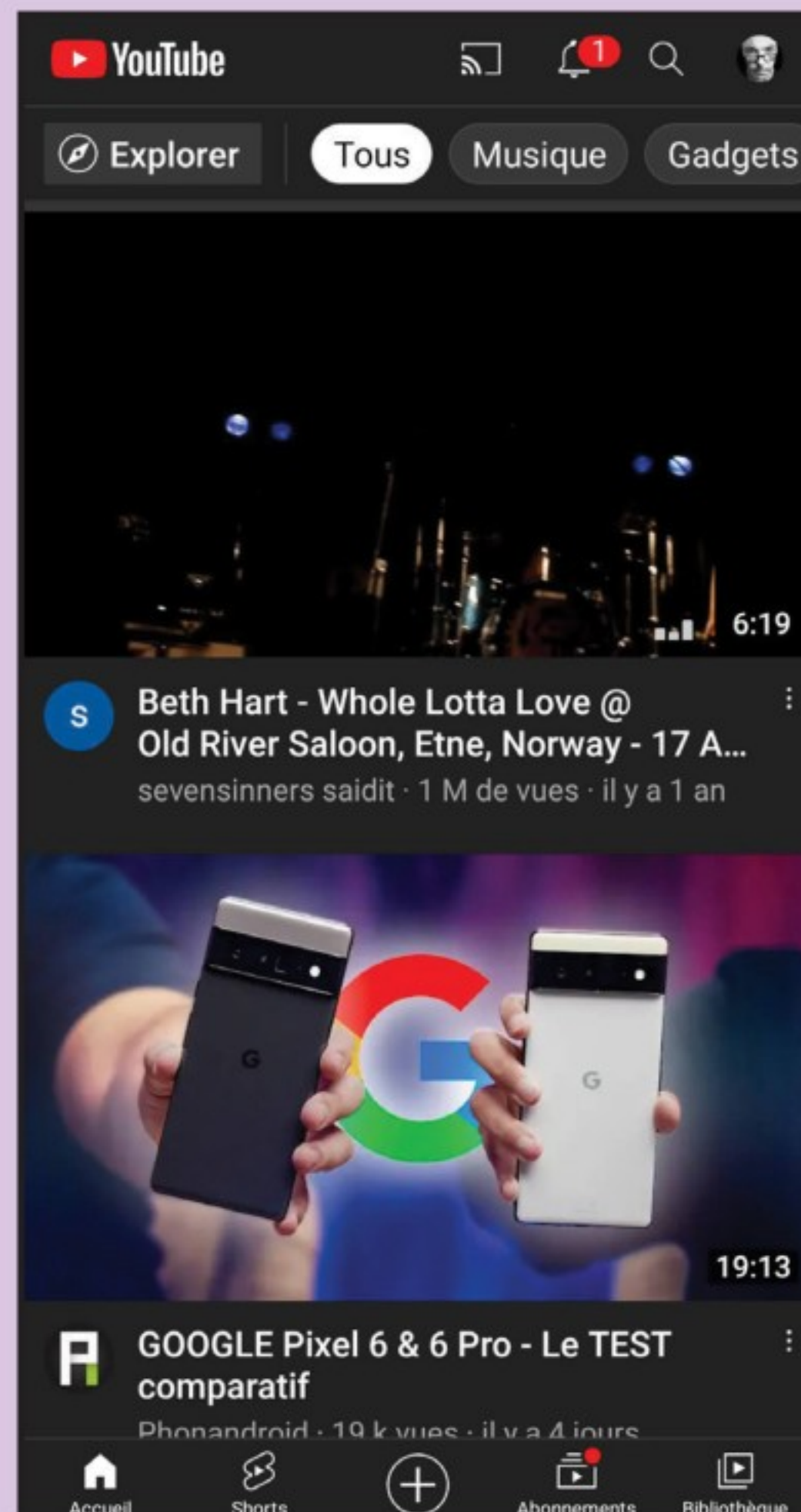


Nous vous présentons YouTube Vanced dans le précédent numéro de Pirate Informatique. Nous

le sélectionnons à nouveau ici, non pas que la protection des données y soit parfaite, mais il s'agit du meilleur rapport qualité/quantité/protection actuel. Un véritable clone de YouTube Premium, sans publicité ciblée et avec les options premium (lancer la lecture d'une vidéo, basculer sur une autre application ou même mettre le smartphone en veille sans interrompre la diffusion du contenu)... mais entièrement gratuit. Ce Mod conserve votre compte et vos listes de lecture.

Inutile de vous ruer tout de suite sur le PlayStore pour rapatrier YouTube Vanced. L'application n'y figure évidemment pas puisqu'elle reprend trait pour trait l'appli officielle de Google tout en privant ce dernier de tout revenu publicitaire lié à l'utilisation de son service. Pour vous profiter de YouTube Vanced, il faudra vous procurer son APK auprès de son éditeur puis l'installer sur votre mobile Android (celui-ci n'a pas besoin d'être rooté pour que l'appli fonctionne).

Lien : vancedapp.com



PLAYSTORE

> Passez à F-DROID



Les possesseurs de smartphones sous Android sont obligés de passer par un compte Google pour profiter des applications les plus connues : Gmail, YouTube, Drive, Photos, etc. Obligés ? Pas vraiment... Promu par la Free Software Foundation, F-Droid propose des applications qui peuvent être installées à la manière du Play Store, mais vous pouvez aussi les télécharger depuis le site au format APK. Ce magasin est utilisé par diverses variantes d'Android comme Replicant, LineageOS et OmniROM.

Le fabricant de smartphones écoresponsables et anti obsolescence programmée Fairphone recommande F-Droid à leurs clients. Pour utiliser ce magasin, il suffit d'aller sur le site officiel et de scanner le QR Code pour télécharger l'appli qui vous donnera accès à toutes les autres. Vous ne trouverez qu'un choix limité d'applications (euh, près de 4500 quand même...) mais elles sont toutes validées par la FSF en terme de sécurisation et répondent à la majorité de nos besoins mobiles, hormis la composante « Réseaux sociaux ».

Lien : f-droid.org

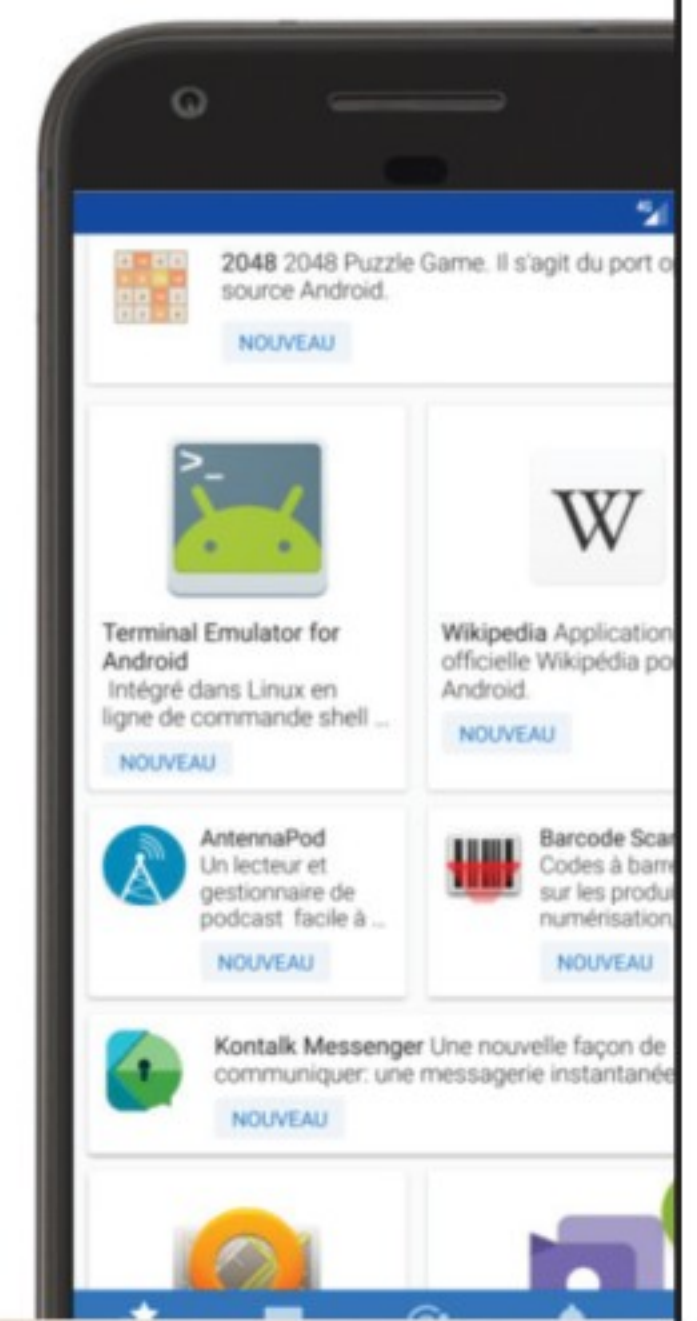


Qu'est-ce que F-Droid ?

F-Droid est un catalogue installable d'applications libres et à code source ouvert sur plateforme Android. Le client facilite la découverte, l'installation et le suivi de vos applications sur votre appareil Android.

TÉLÉCHARGER F-DROID

Signature PGP





POUR QUI ?

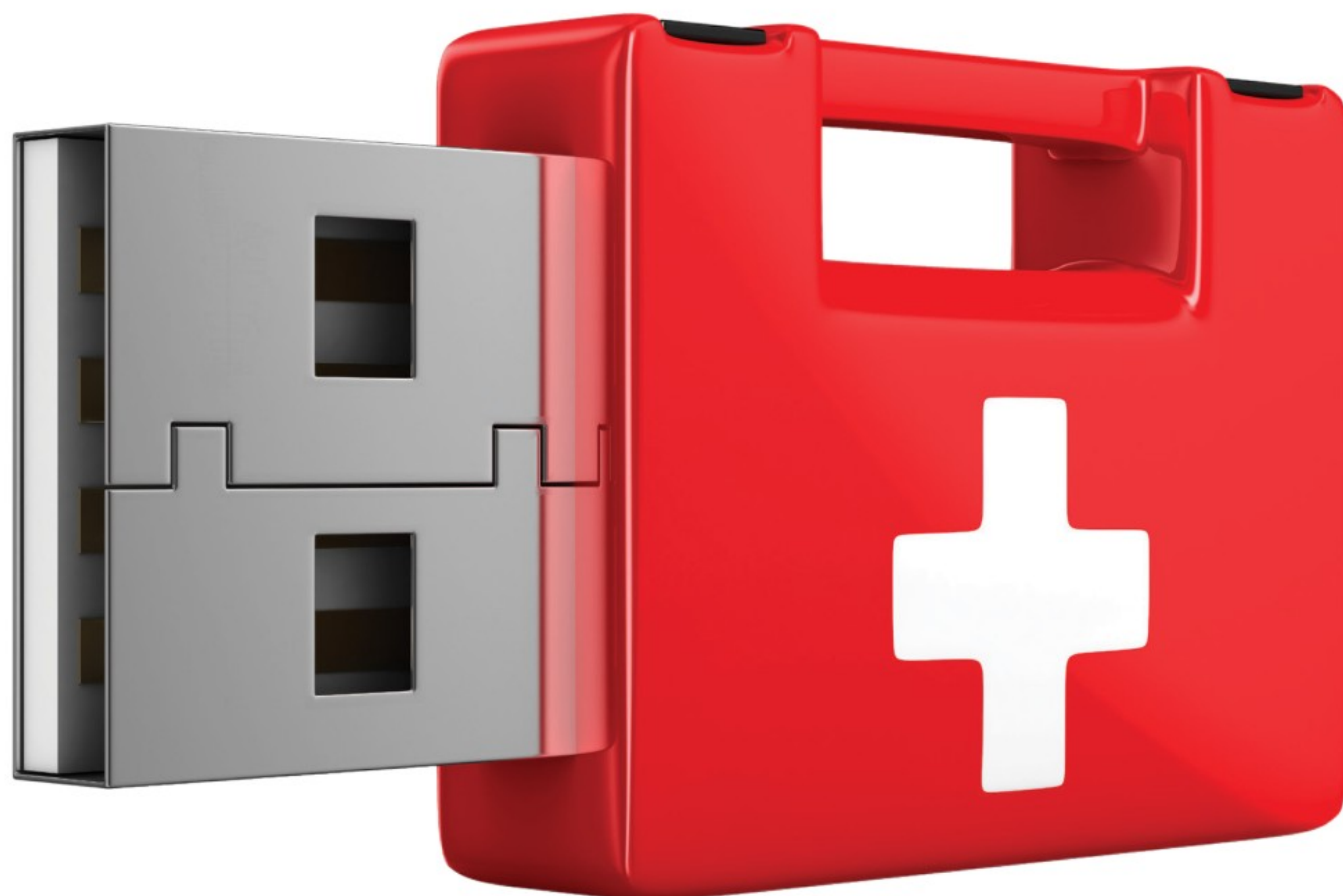
Pour les
prévoyants et
suspicieux

POUR QUOI FAIRE ?

Détecter un
malware qui
aurait déjoué
votre antivirus
principal ou
disposer d'un
outil d'analyse
extérieure en cas
de problème

CONSERVEZ UN ANTIVIRUS À PORTÉE DE MAIN

Vous avez des doutes sur l'efficacité de l'antivirus installé sur votre PC et soupçonnez la présence d'un intrus sur votre machine. Préparez une clé de secours pour en avoir le cœur net.



Les pirates et les éditeurs de logiciels antivirus se livrent une guerre sans fin. Les premiers ayant toujours une longueur d'avance, votre logiciel antivirus installé sur votre PC ne détecte peut-être pas tout ce qui transite par le Web et fini par rejoindre votre disque dur lors d'un téléchargement. Plutôt fourbes, certains malwares prennent parfois la main sur l'antivirus afin d'éviter que celui-ci ne les détecte. Pour contrer le phénomène, mieux vaut procéder à une vérification régulière de votre machine en lançant une analyse anti-malware s'appuyant sur un autre outil. C'est l'objet de Emsisoft Emergency Kit

UN ANTIVIRUS TOUJOURS PRÊT

L'outil gratuit fourni par Emsisoft présente deux avantages. D'abord, il arrive en complément de l'antivirus installé sur votre PC et ne s'y substitue pas. Ensuite, il peut être lancé depuis un second disque dur ou même une clé USB. Un aspect pratique si vous devez analyser plusieurs PC, les vôtres, mais aussi ceux de vos proches. À noter qu'à chaque lancement, ce kit de secours effectue une mise à jour afin de collecter les signatures de virus les plus récentes. Il vous permet aussi d'opérer des analyses plus ou moins complètes selon le temps dont vous disposez devant vous.



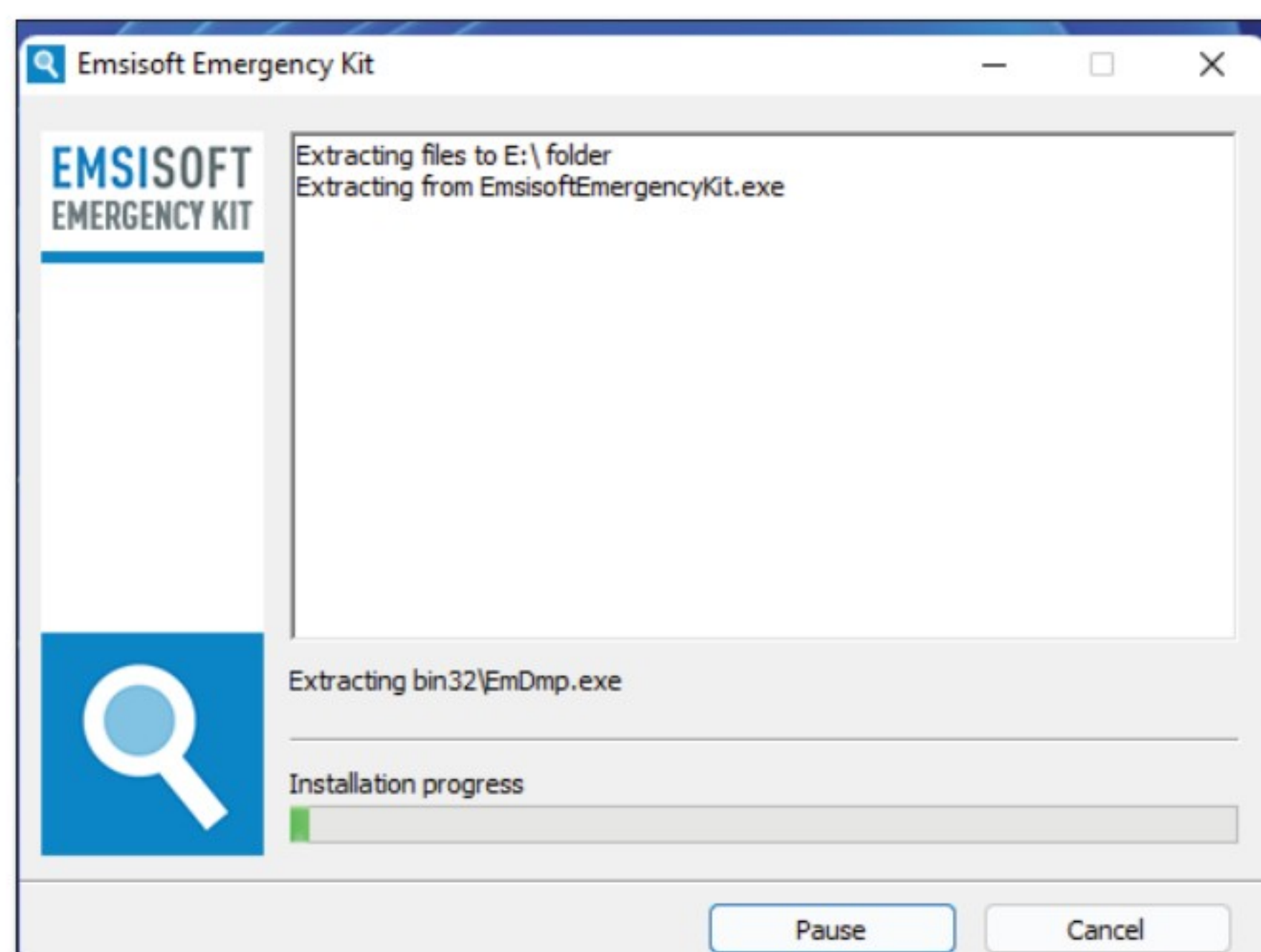
ANALYSE AVEC EMSISOFT EMERGENCY KIT

PRATIQUE



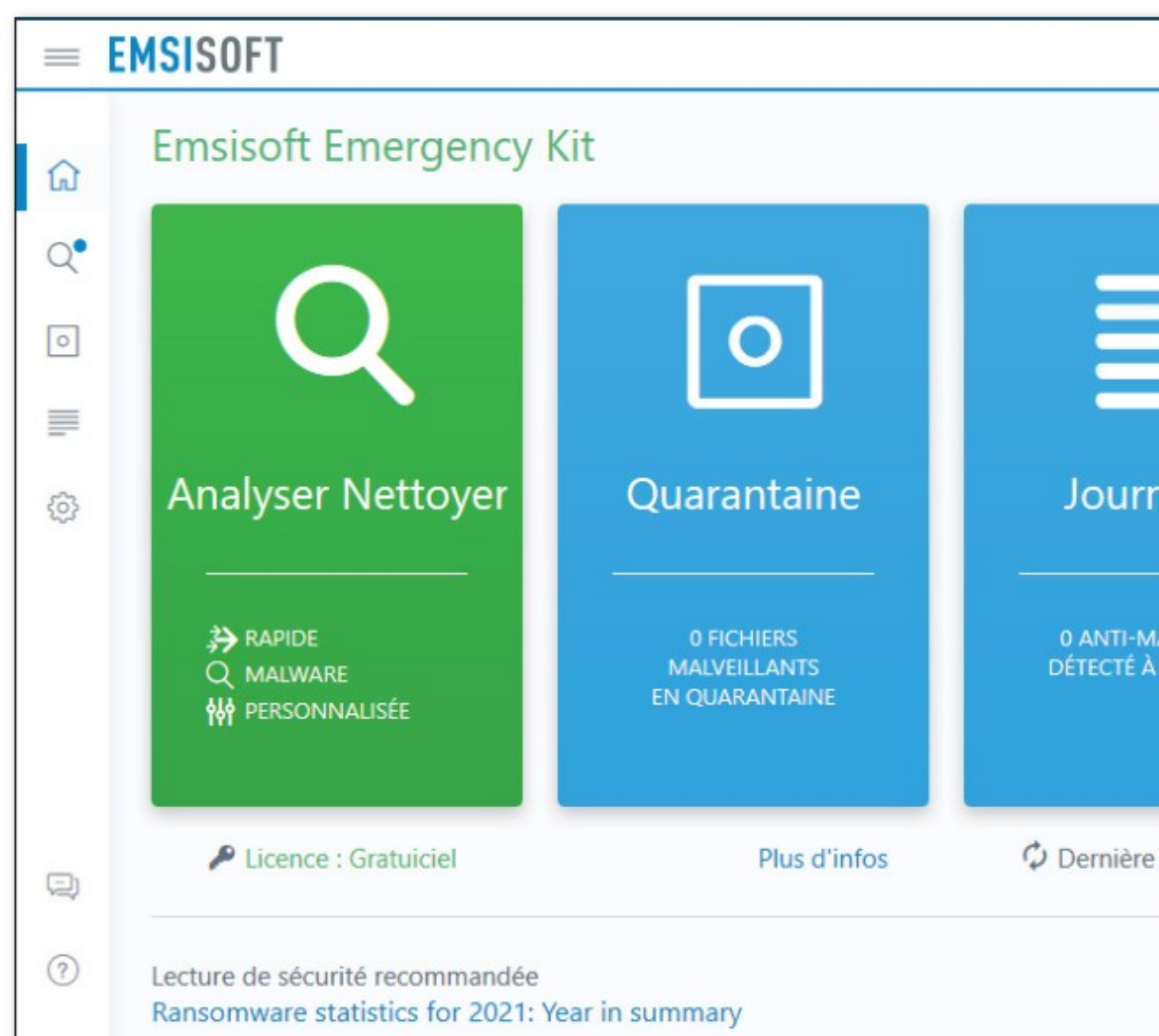
01> INSTALLER L'OUTIL

Téléchargez le logiciel gratuit puis lancez son installation en prenant soin de désigner un autre disque que le disque système (un second disque dur, un disque externe ou une clé USB par exemple). Une fois l'opération effectuée, l'Emergency Kit procède à une mise à jour de sa base de signatures. Veillez à disposer d'une connexion Internet à ce moment-là.



02> CHOISIR LE TYPE D'ANALYSE

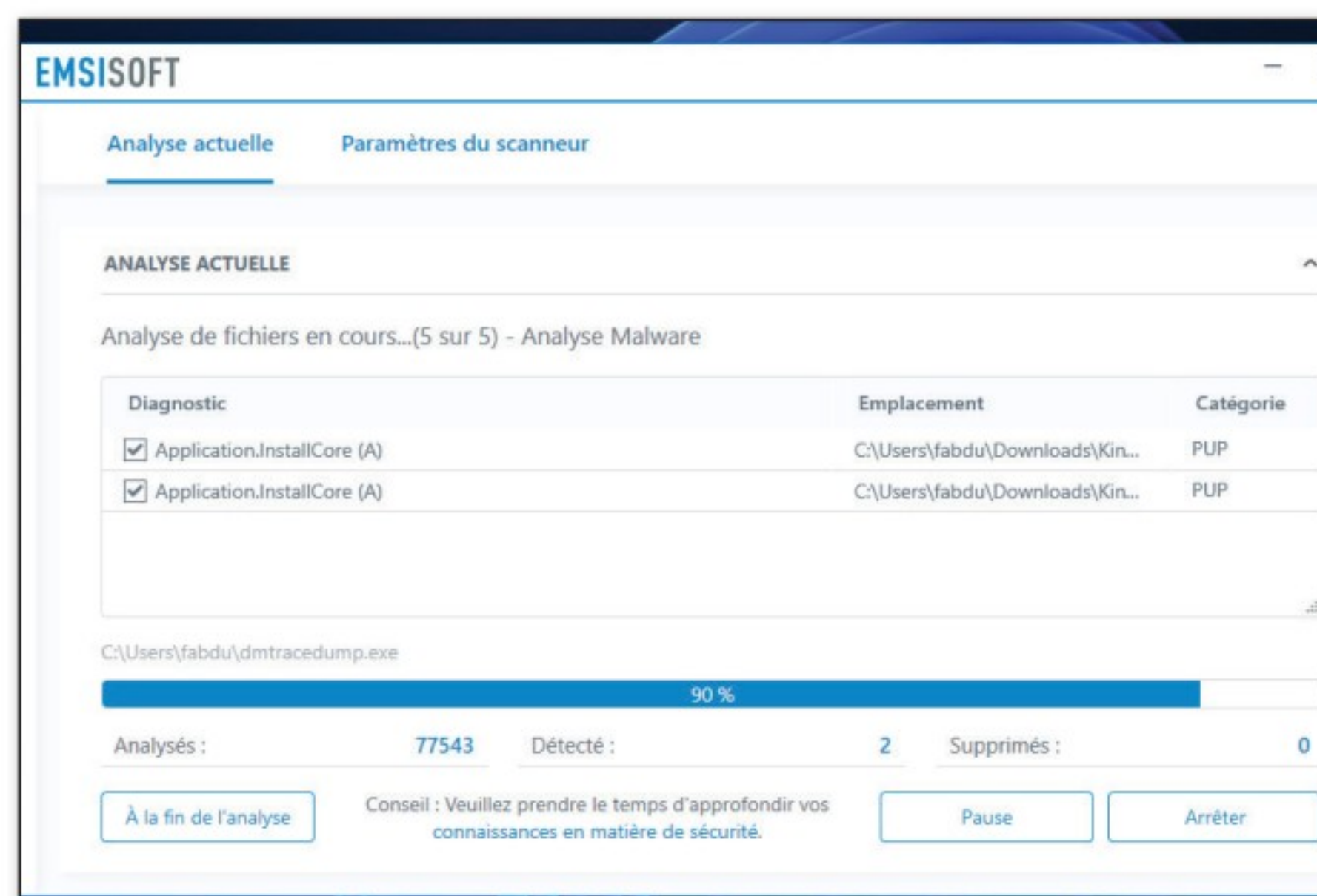
Lorsque tout est prêt, la première rubrique, **Analyser Nettoyer**, passe en vert. Trois types d'analyse sont alors proposés : **Rapide**, pour un balayage express du contenu du disque dur, **Malware** pour cibler spécifiquement les dossiers prisés par les malwares et **Personnalisée**.



Cette dernière méthode permet d'exclure du scan les dossiers que vous souhaitez. Cliquez sur le mode qui vous convient.

03> VÉRIFIER LES RÉSULTATS

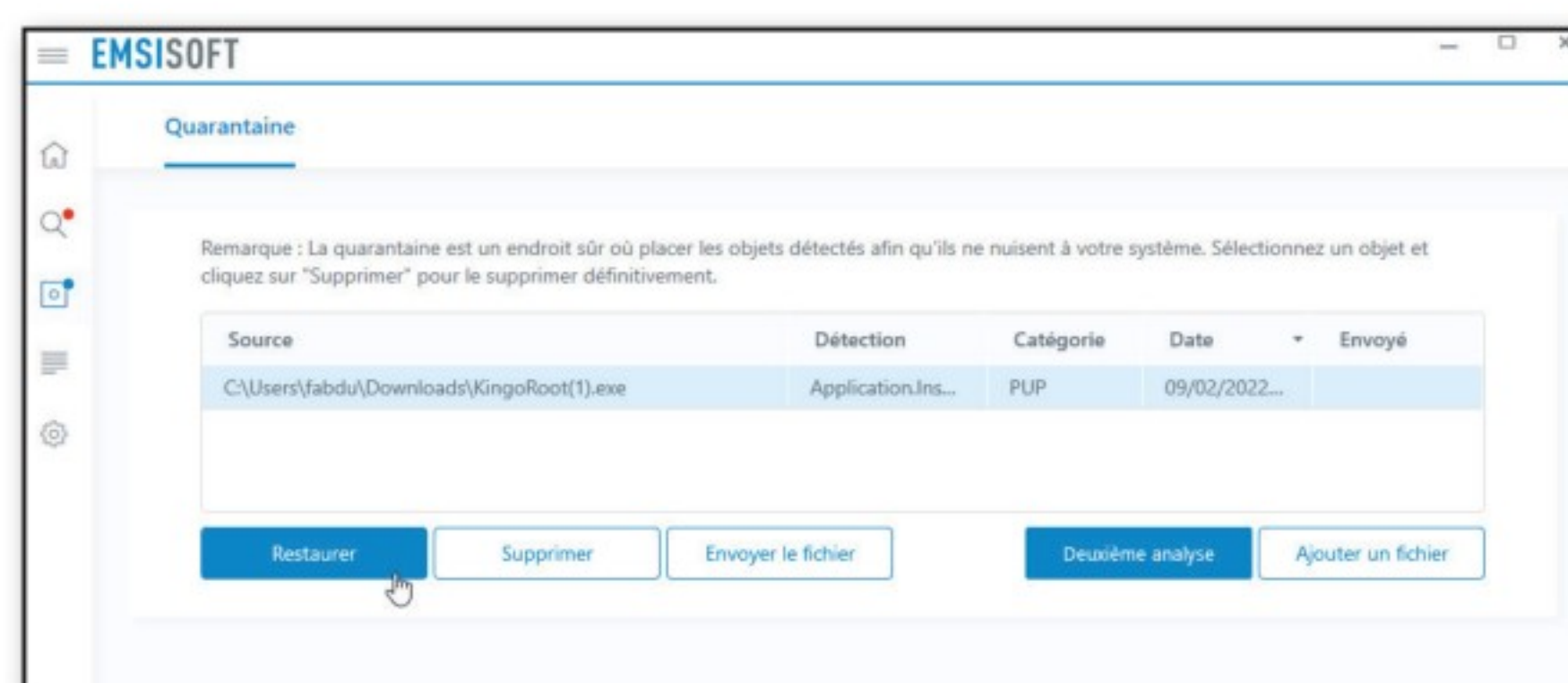
L'analyse démarre (le mode Malware dans notre exemple) et signale au fur et à mesure les intrus détectés. Lorsqu'elle est terminée, et si des problèmes sont apparus,



Emsisoft propose évidemment de lui confier la surveillance antivirus de votre machine à la place du logiciel que vous utilisez (et qui a laissé passer des intrus). Cliquez sur **Fermer**.

04> PRENDRE LES BONNES DÉCISIONS

Si des intrus ont été repérés, ils figurent dans le rapport de diagnostic. À vous de décider si vous souhaitez les éliminer ou simplement les placer en quarantaine. Cochez



la case en regard du nom du malware ou du logiciel potentiellement indésirable (PUP) et faites votre choix. Si vous le placez en quarantaine, vous pourrez le remplacer à son emplacement d'origine en cliquant sur **Quarantaine** à gauche puis sur **Restaurer**.





PIXELS- ESPIONS :

QUAND VOS EMAILS SONT SURVEILLÉS

Alors que les sites Web sont tenus de vous informer des cookies qu'ils déposent sur votre PC et des données collectées lorsque vous les visitez, la messagerie électronique reste encore le Far West de la surveillance dissimulée.

Vous recevez probablement plusieurs dizaines de mails au quotidien à travers vos différentes messageries comme Gmail, Outlook ou encore Yahoo par exemple. Nombre d'entre eux émanent de sites marchands dont vous êtes client ou sur lesquels vous avez laissé vos coordonnées, notamment votre adresse email.

Ces campagnes d'emailing seraient bien vaines si le commerçant en question, ou la régie publicitaire qui s'en occupe, ne pouvait avoir un retour sur son efficacité. Pour cela, il existe une technique simple et efficace : le pixel-espion. Également appelé Tracking pixel ou encore pixel invisible, le pixel-espion se niche dans de nombreux emails que vous recevez, et ce sans que vous ne vous en rendiez compte. Selon une étude menée l'an passé par

Basecamp l'éditeur américain de la messagerie Hey, près des deux tiers des mails qui arrivent dans nos boîtes de réception contiennent des mouchards.

Près des deux tiers des mails qui arrivent dans nos boîtes de réception contiendraient des mouchards.

CAPE D'INVISIBILITÉ

Pour passer inaperçu, le pixel-espion prend la forme d'un élément graphique, en général une image, mais il peut aussi s'agir d'un Gif, transparent et ne mesurant qu'un pixel de côté. Il est donc complètement indétectable à l'œil. Cependant, il a beau être minuscule, il n'en demeure pas moins des plus efficaces pour renseigner la marque, le commerçant ou la régie publicitaire, sur votre activité. Il peut ainsi livrer des informations sur l'heure de l'ouverture de l'email et le temps passé à sa lecture, le navigateur et le système d'exploitation utilisés, le matériel (ordinateur, smartphone ou tablette), l'adresse IP (et donc la localisation) et bien sûr si l'utilisateur a cliqué sur un lien figurant dans l'email et lequel.

Autant d'informations qui permettent d'affiner le ciblage et d'améliorer les campagnes marketing sans pour autant en informer le client final. Si le Règlement général sur la protection des données (RGPD) est globalement bien respecté sur le Web, il reste encore assez peu appliqué aux emails. Car les pixels-espions ne se contentent pas de se loger dans les messages électroniques. Ils sont également très appréciés sur les sites Web où, associés à des cookies, ils peuvent transmettre encore plus de données



Si le Règlement général sur la protection des données (RGPD) est globalement bien respecté sur le Web, il reste encore assez peu appliqué aux emails.

pour améliorer le ciblage publicitaire et alimenter des statistiques sur le parcours du visiteur. Mais dans ce cas, le consentement de l'utilisateur doit être demandé.

COLLECTER POUR MIEUX CIBLER

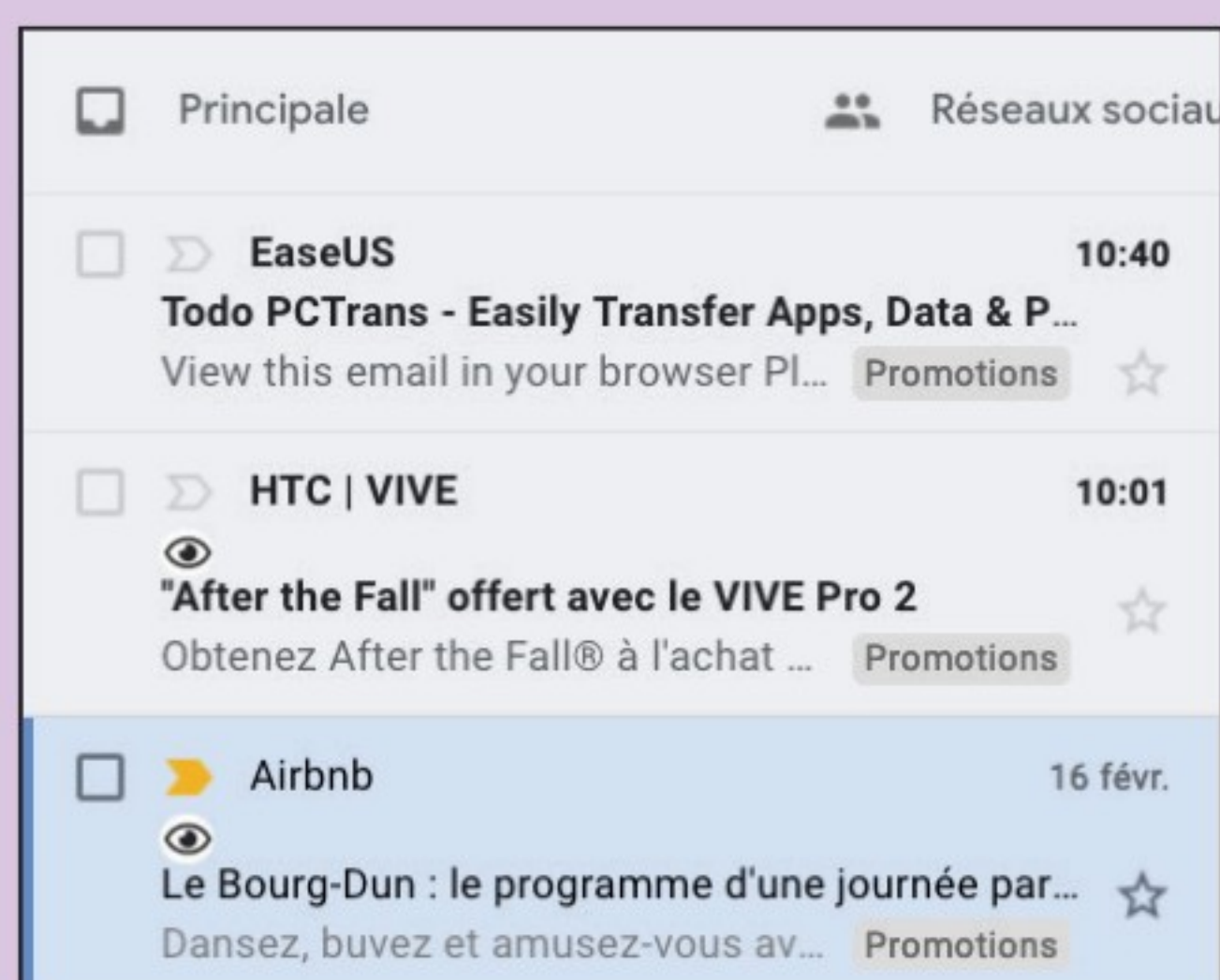
Le fonctionnement d'un pixel-espion est à la fois simple et redoutable. Pour s'afficher (bien qu'il soit transparent, il est bel et bien présent), il va être téléchargé depuis un serveur qui, du coup, sera informé de la requête et de sa provenance. Malin. Tout sera alors consigné à des fins de suivi statistique et de ciblage. On retrouve également les pixels-espions dans bon nombre de newsletters. Ils permettent par exemple à l'expéditeur de savoir si celle-ci a été, ouverte, lue et quand. En fonction des résultats, il pourra optimiser le contenu et l'heure d'expédition pour toucher encore plus de monde.

Véritable intrusion dans la vie privée puisqu'ils œuvrent en cachette, les pixels-espions ne sont pas pour autant une fatalité. Il existe plusieurs moyens pour, non pas s'en prémunir, mais tout au moins les démasquer.

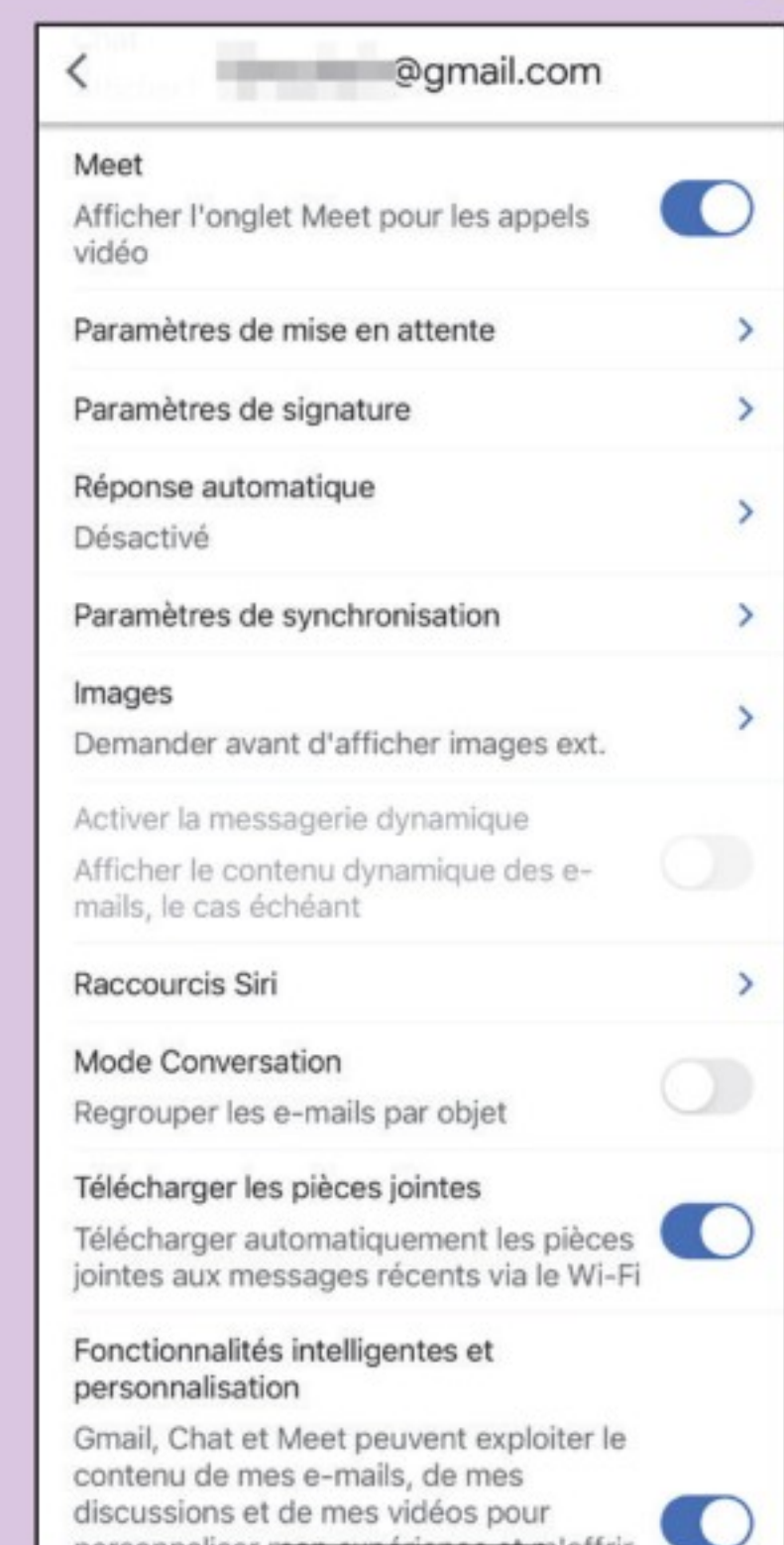
TRAQUEZ ET BLOQUEZ LES PIXELS !



Si vous relevez vos emails avec un navigateur Web (pour Gmail), vous pouvez équiper votre navigateur d'une extension gratuite comme Ugly Email ou PixelBlock. Elles permettent d'avertir de la présence d'un pixel-espion dans les messages avant que ceux-ci ne soient ouverts en affichant une icône en forme d'œil près du nom de l'expéditeur. À vous alors de choisir si vous souhaitez lire ou non le mail en sachant



qu'un traqueur s'y cache. Avec d'autres Webmail ou des logiciels de messagerie, le moyen le plus efficace pour éviter les traqueurs dans les mails, reste d'interdire le téléchargement automatique des images depuis les paramètres du compte ou du logiciel. Microsoft indique pour sa part qu'aucune action de l'utilisateur n'est requise pour empêcher le téléchargement des images. La fonction est activée par défaut par l'éditeur. Sachez enfin que vous pouvez aussi empêcher ce suivi sur vos appareils mobiles iOS et Android.

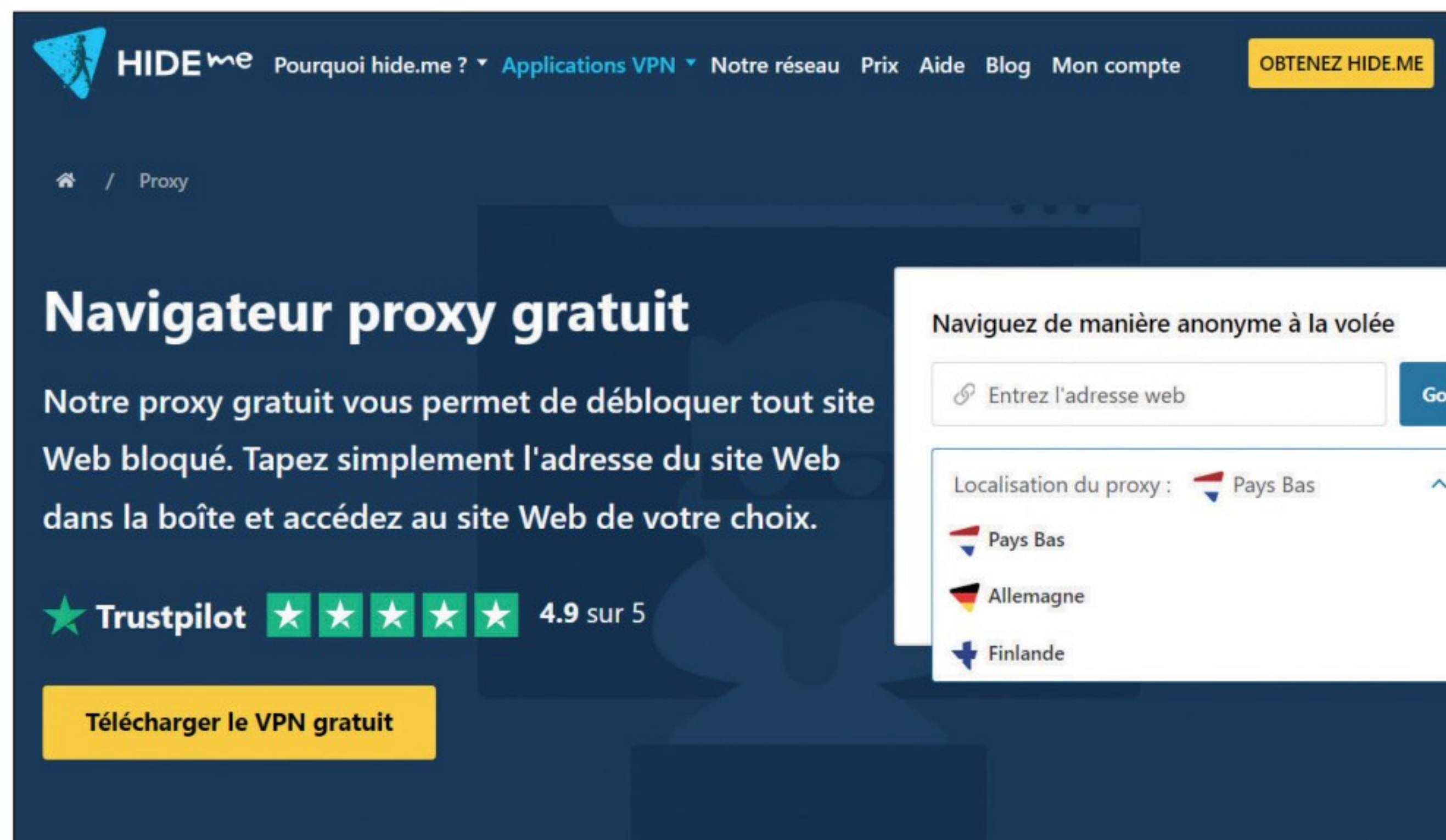




Proxy d'appoint facile > AVEC HIDE ME

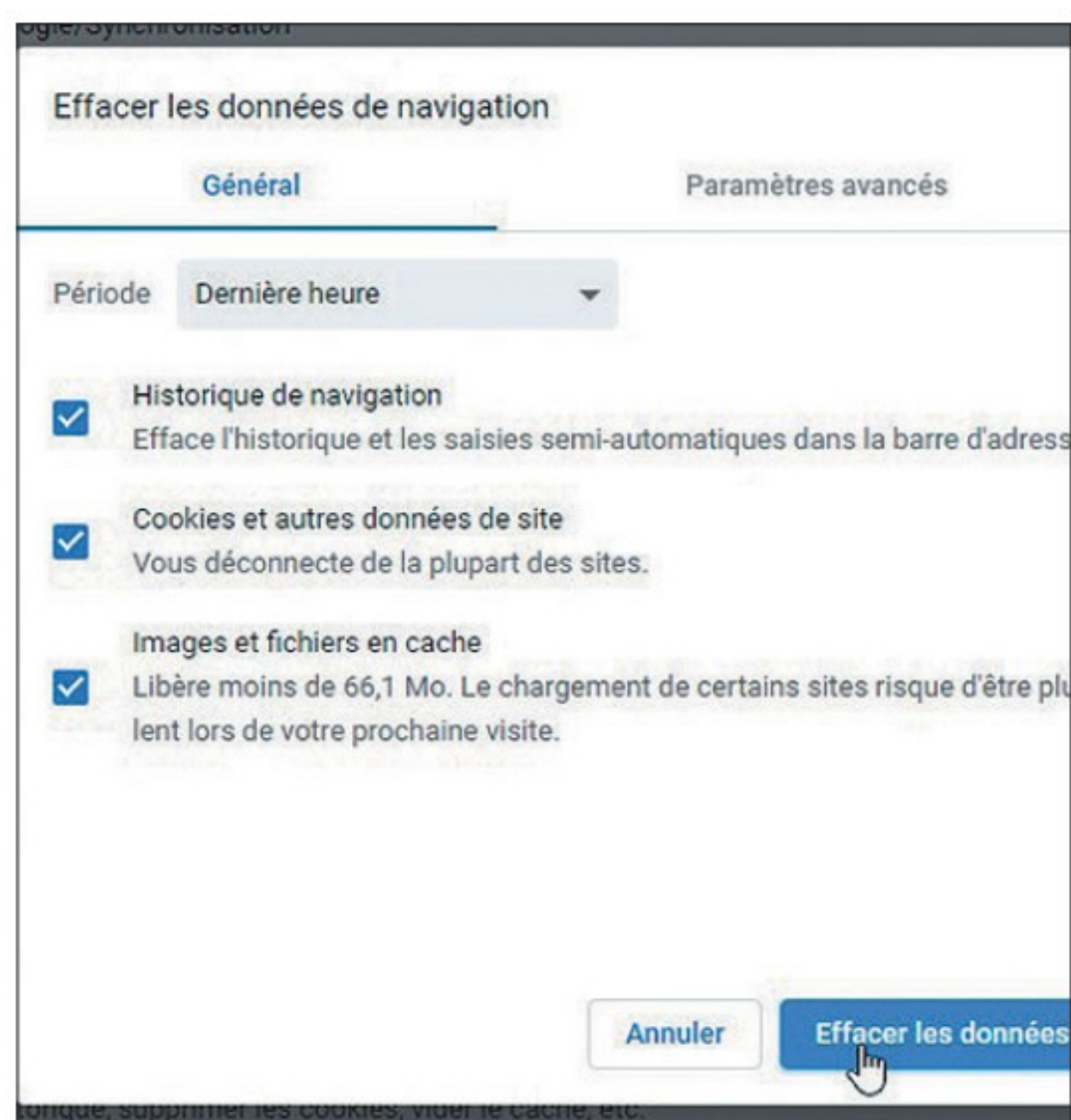
Le service de VPN Hide Me propose un proxy gratuitement, même si vous n'avez pas de compte chez eux. Il suffit de renseigner l'URL du site à visiter et de choisir parmi les trois localisations possible (oui, c'est peu et cela reste en Europe) : Pays-Bas, Allemagne, Finlande. Mais vous bénéficiez de la rapidité et de la fiabilité de Hide Me ainsi que d'options de sécurisation (chiffrement, no script, etc.). Un proxy d'appoint ultra-simple et efficace.

Lien : hide.me/fr/proxy



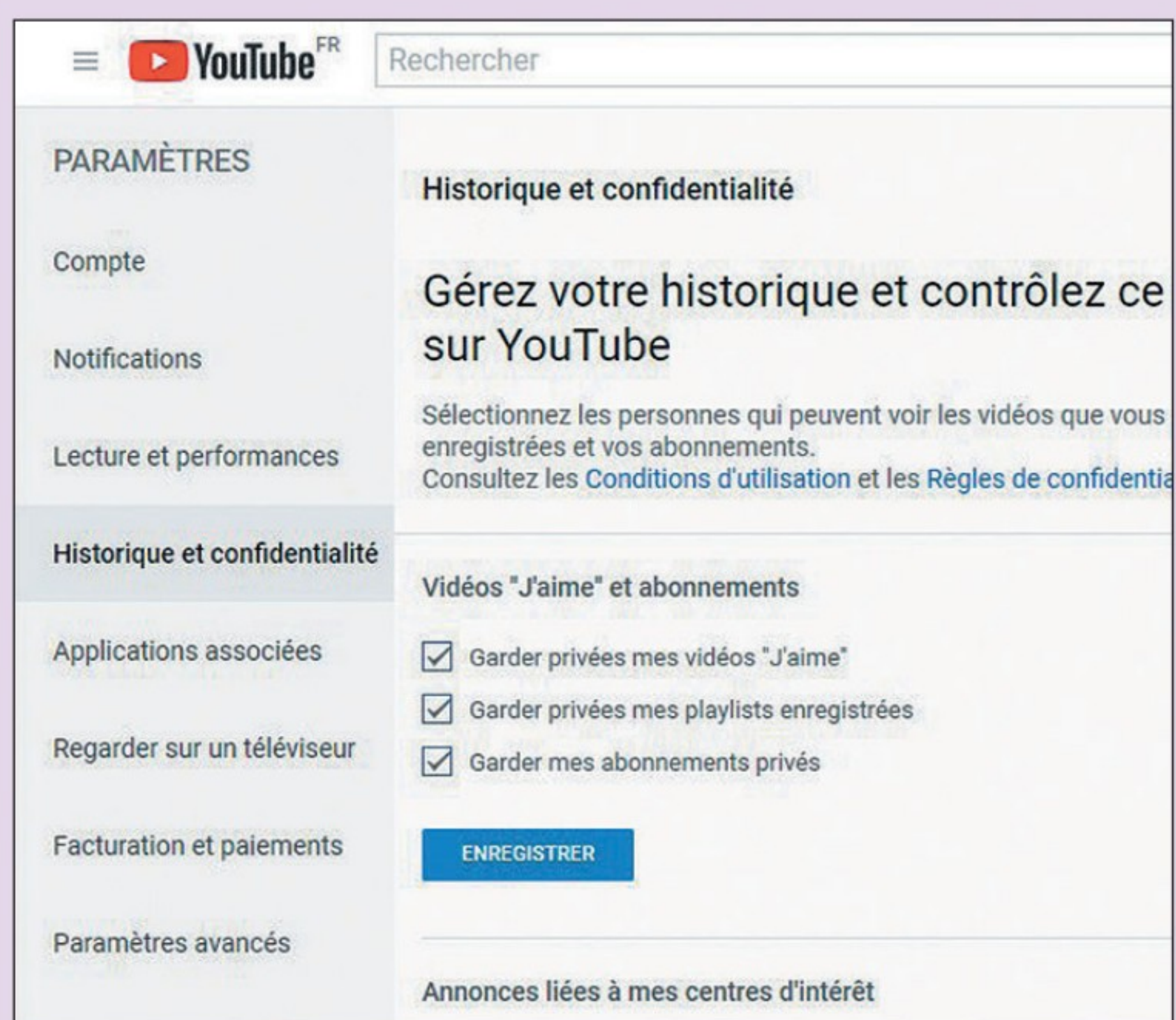
Effacer votre historique > AVEC CHROME

L'historique et les cookies permettent de savoir quels sites vous avez visités, voire même de se connecter à vos comptes sans vérification d'identité (voir « Penser à se déconnecter »). Vous pouvez effacer tout cela dans les **Paramètres** de Chrome (via les 3 petits points en haut à droite), dans **Confidentialité et sécurité > Effacer les données de navigation**. Il y a aussi un raccourci clavier bien pratique : tapez la combinaison de touches **Ctrl + Maj + Suppr.**



Masquer ses abonnements > AVEC YOUTUBE

À Vos abonnements à des chaînes YouTube sont a priori visibles par tous les autres internautes. Si vous souhaitez les garder privés, connectez-vous à votre compte, rendez-vous dans les **Paramètres** YouTube (cliquez sur votre avatar puis sur la roue crantée). Dans **Confidentialité**, cochez la case **Garder mes abonnements privés**. Validez avec **Enregistrer**.



Oui, recycler mes papiers, c'est utile.

Pour l'environnement

Le recyclage des papiers permet **d'économiser les matières premières et l'énergie.**



Le recyclage de papier, c'est :

💧 💧 💧 **3 fois** moins d'eau*

⚡ ⚡ ⚡ **3 fois** moins d'énergie*

* comparé à la fabrication de papier non recyclé

Pour l'emploi

La filière du recyclage des papiers **en France, c'est 90 000 emplois non délocalisables.**



Collecte



Papeterie



Centre de tri



Découvrez le recyclage du papier
sur www.consignesdetri.fr

CITEO

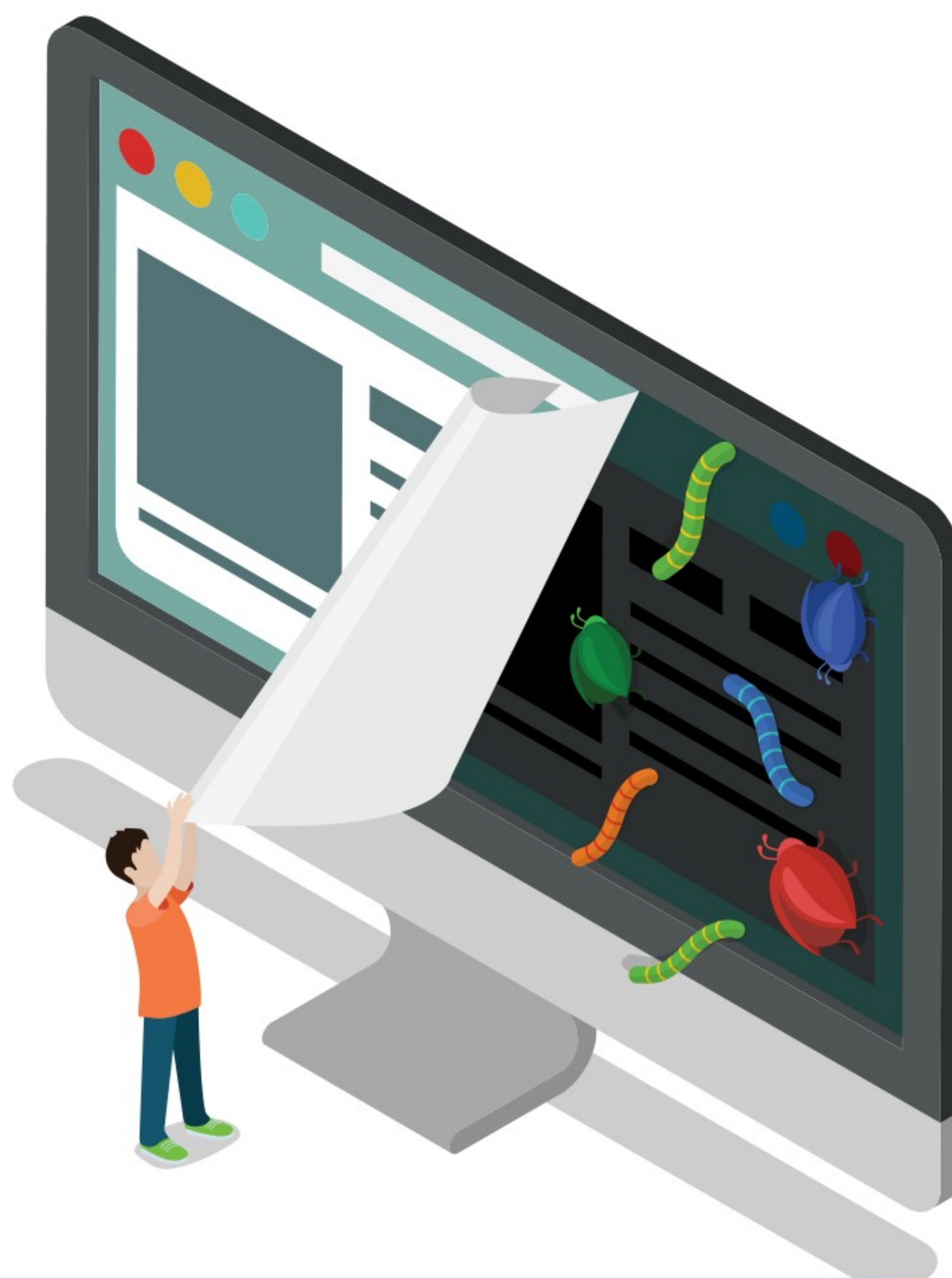
Le nouveau nom
d'Eco-Emballages et Ecofolio



COMMENT DÉTECTER ET SE PROTÉGER DES SITES FRAUDULEUX ?

Pas besoin d'être à Pâques pour le savoir : il y a plus d'arnaques sur internet que de chocolats dans votre salon ! Ne soyez pas cloche : des plateformes de vérification existent en cas de doute sur un site ou un service.

Plus de 1,5 million de Français sont victimes d'arnaques via internet chaque année. Et cela sans compter ceux qui n'osent pas en parler. Le site cybermalveillance.gouv.fr permet bien de les signaler, voire d'obtenir des conseils pour résoudre certains soucis, mais ce serait encore mieux de ne pas se faire avoir, non ? Pour prévenir plutôt que de n'offrir qu'un mur des lamentations, le gouvernement français vient d'entériner au parlement la création un nouvel outil le 24 février dernier : baptisée Cyberscore, cette plateforme notera la sécurité et la fiabilité des sites et services pour que les internautes puissent être éclairés en cas de doute. À la manière d'un Nutriscore, les sites visés devront réaliser un audit portant notamment sur la sécurisation et la localisation des données hébergées. Les réseaux



Nous pouvons tous prendre du temps pour vérifier les signaux d'alerte qui existent sur n'importe quel site dangereux. Mais honnêtement, qui le fait ? Heureusement, des services en ligne font ce travail pour nous.

LES BONS RÉFLEXES À ADOPTER



Si vous ne connaissez pas un site, posez-vous les bonnes questions avant de passer commande.

1. Vérifiez son propriétaire via Whois ou Afnic.
2. Utilisez les outils de sécurité de votre navigateur : s'il vous prévient qu'un site est dangereux, n'insistez pas.
3. Utilisez des outils de sécurité. Des extensions, mais aussi des sites internet dédiés, vérifient chaque jour la sécurité des pages que vous pourriez visiter.
4. Certains éléments doivent tout de suite attirer votre attention :
 - Un site marchand non sécurisé (avec http au lieu de https dans sa ligne d'adresse)
 - Des mentions légales et/ou Conditions générales de vente (CGV) inexistantes ou mal formulées
 - Une url qui ne correspond pas à celle de la marque
 - Des pop-up dans tous les sens qui tentent de vous rediriger ailleurs
 - Des fautes d'orthographe un peu trop fréquentes.

sociaux et principaux sites de visioconférence devraient être les premiers concernés. Ce dispositif n'entrera cependant en vigueur qu'en octobre 2023. Chaque année, de nouvelles formes d'arnaque viennent au monde. Il y a les mails douteux, le dropshipping, les sites qui jouent à la marchande, mais ne vous envoient jamais leurs produits, ceux qui s'amusent un peu trop à siphonner vos données... Et il faut bien reconnaître que scruter chaque site pour chercher ses mentions légales, les analyser, puis vérifier s'il y a des avis en ligne, peut vite s'avérer un peu... usant. Vous n'êtes pas arrivé à l'heure de la 5G pour étudier tous les nouveaux sites en prenant autant de temps qu'à l'époque des modems ! Heureusement, il existe d'autres solutions que de tirer à pile ou face avant de passer une commande.

D'AUTRES OUTILS DE VÉRIFICATION

Vous n'avez pas envie d'attendre jusqu'en 2023 pour valider les sites que vous visitez ? Vous avez bien raison. D'autant que le Cyberscore n'évoque pas, pour le moment, l'e-commerce. Ni même les sites qui ressemblent étrangement à ceux d'enseignes existantes, mais qui pratiquent le phishing, que vous soyez ou non un gros poisson. Que faire alors, direz-vous, paniqué à l'idée de vous faire arnaquer ? Entre labels, sites communautaires et extensions pour navigateurs, vous avez heureusement le choix.



CYBER-SCORE



IL FAUDRA ATTENDRE 2023 POUR QUE LA PLATEFORME FRANÇAISE CYBERSCORE, CRÉÉE PAR L'ÉTAT FRANÇAIS, NE VOIE LE JOUR. SUR LE MÊME MODÈLE QUE LE NUTRIScore, L'IDÉE EST DE DONNER UNE NOTE « CYBERSÉCURITÉ » AUX SITES WEB QUE NOUS VISITONS. EN ATTENDANT, D'AUTRES SOLUTIONS EXISTENT DÉJÀ.



LES LABELS, UN GAGE DE SÉRIEUX ?



Il fut une époque où les sites marchands affichaient de jolis petits labels en bas de leurs pages. Fia-Net, Webcert et autres étaient mis en avant. La plupart ont maintenant disparu, même si vous pouvez encore les retrouver ici ou là. Aujourd'hui, hélas, ils ne constituent plus un sceau de qualité : il est trop facile de reproduire un logo et de l'insérer sur un site pour s'approprier sa renommée. Par contre, il peut être plus intéressant de lire des avis clients certifiés par NF Service ou Trust Pilot, même s'ils ne peuvent pas totalement garantir leur véracité.

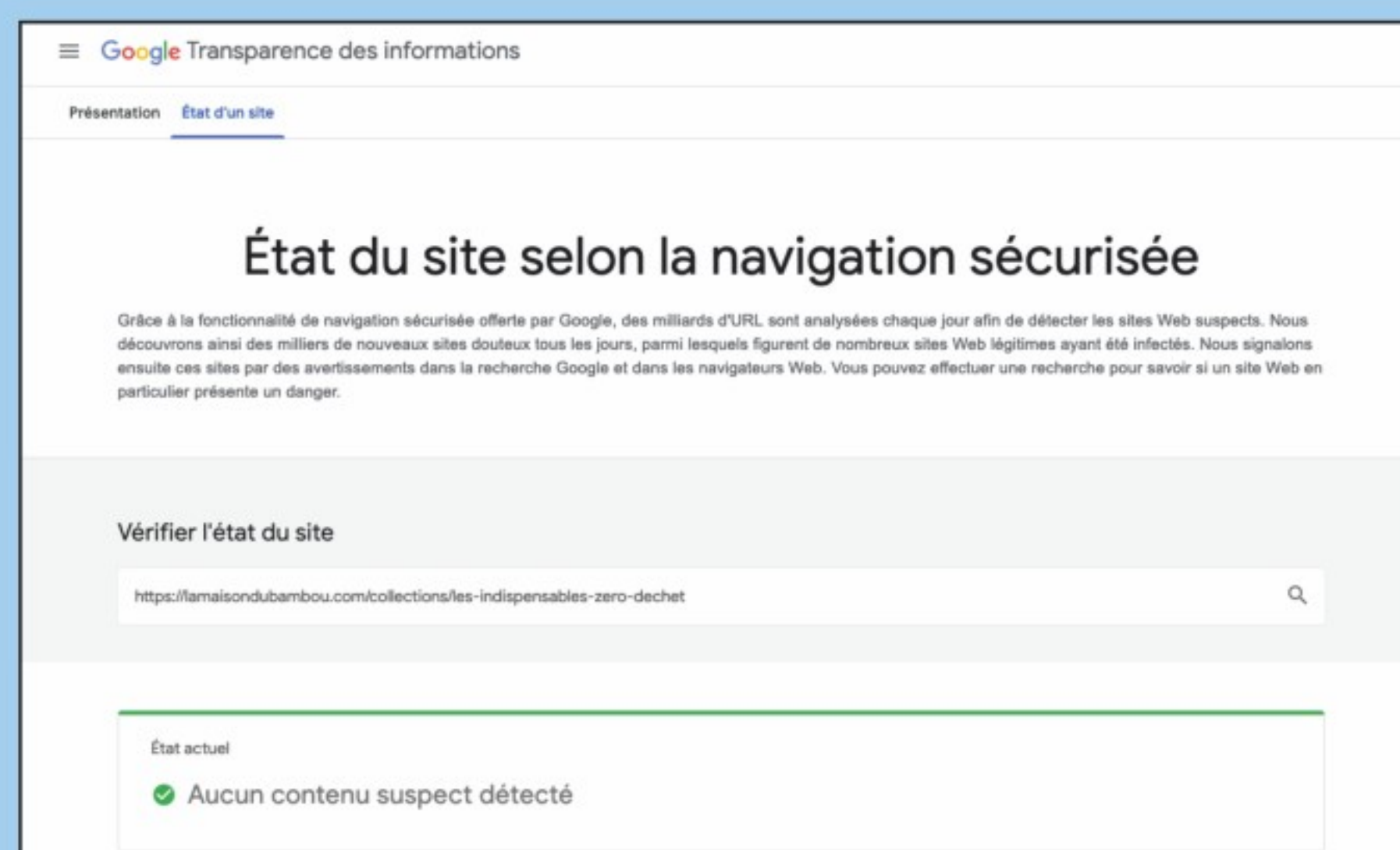


TOP 5 DES OUTILS DE VÉRIFICATION

TRANSPARENCY REPORT, PAR GOOGLE

Qui de mieux que le géant d'internet pour vérifier la sécurité d'un site internet. Des milliards d'URL sont analysées quotidiennement afin de détecter les sites Web suspects, dont des milliers de nouveaux sites douteux chaque jour, parmi lesquels figurent de nombreux sites Web légitimes ayant été infectés. Vous pouvez effectuer une recherche pour savoir si un site Web en particulier présente un danger. Attention, cependant : il vous renseignera bien sur le potentiel malveillant d'un lien. Mais il ne vous dira rien sur sa fiabilité commerciale.

Lien : <https://bit.ly/3huL7E4>



CAPTAIN DROP, CONTRE LE DROPSHIPPING

Arrêtez de payer quatre fois le prix pour des produits provenant de Chine ! Le petit chien renifleur de Captain Drop vérifie les sites et vous indique également où vous pourrez trouver les mêmes produits... mais étrangement pour beaucoup moins cher. Il est disponible en ligne ou via une application pour smartphone.

Lien : fr.captaindrop.com

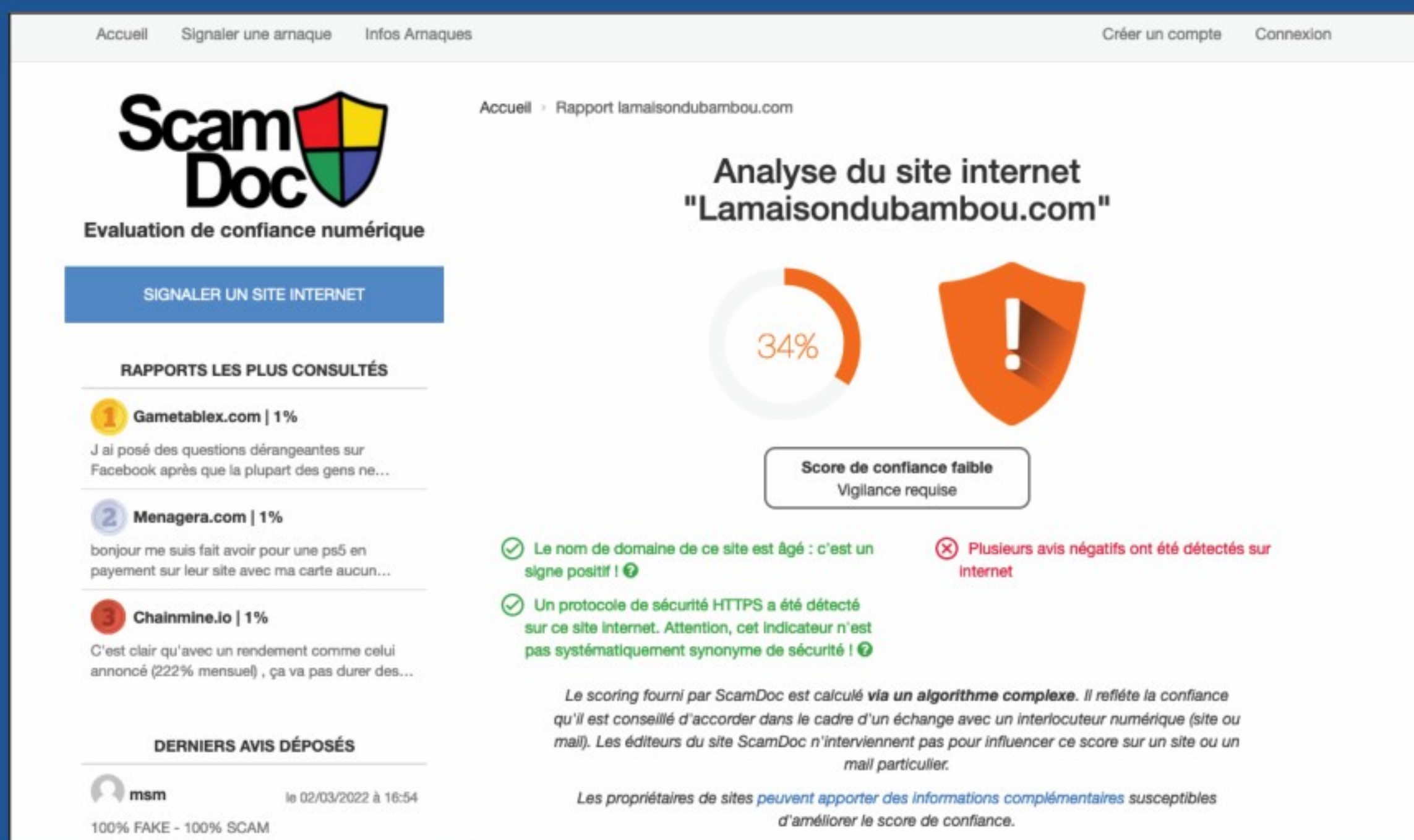


SCAMDOC, POUR CONNAÎTRE LE RETOUR D'AUTRES UTILISATEURS

Vous voulez savoir quels sont les avis généraux concernant un site ? Parce qu'il peut être très long et complexe de collecter des données fiables (ancienneté, avis négatifs, identité du propriétaire du site, espérance de vie du site...), il y a désormais un réflexe très simple à adopter : consulter ScamDoc. Le site s'appuie sur de multiples sources de données et du machine learning pour fournir son évaluation. Il permet ainsi de faire gagner un temps considérable aux internautes qui recherchent des avis en ligne. Avec une limite cependant :

l'analyse ne repose que sur les avis qu'il a pu enregistrer. Cette dernière peut donc être assez restreinte ou nulle pour de nouveaux sites, même si elle s'appuie aussi sur des éléments plus concrets comme l'identité des propriétaires.

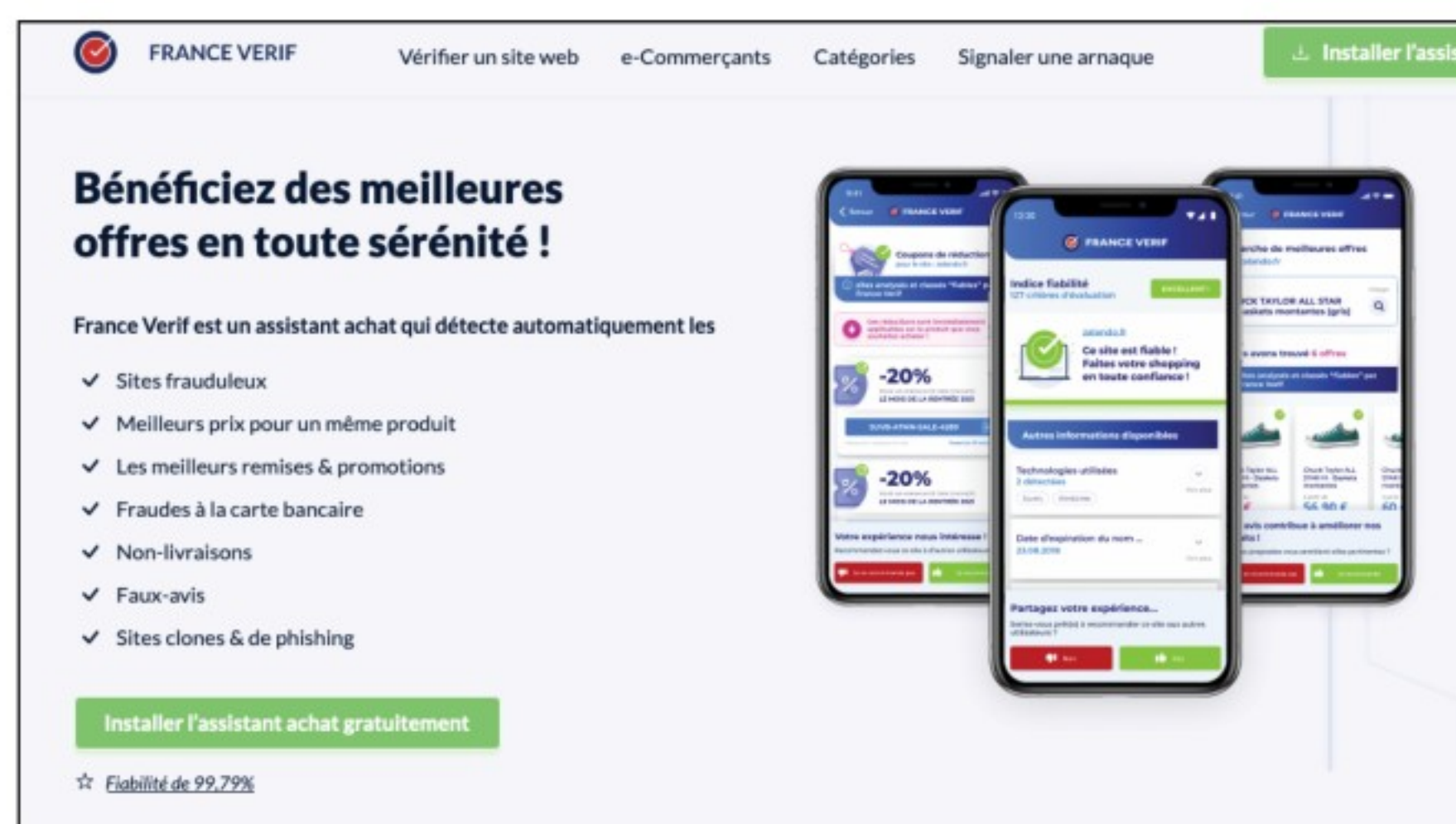
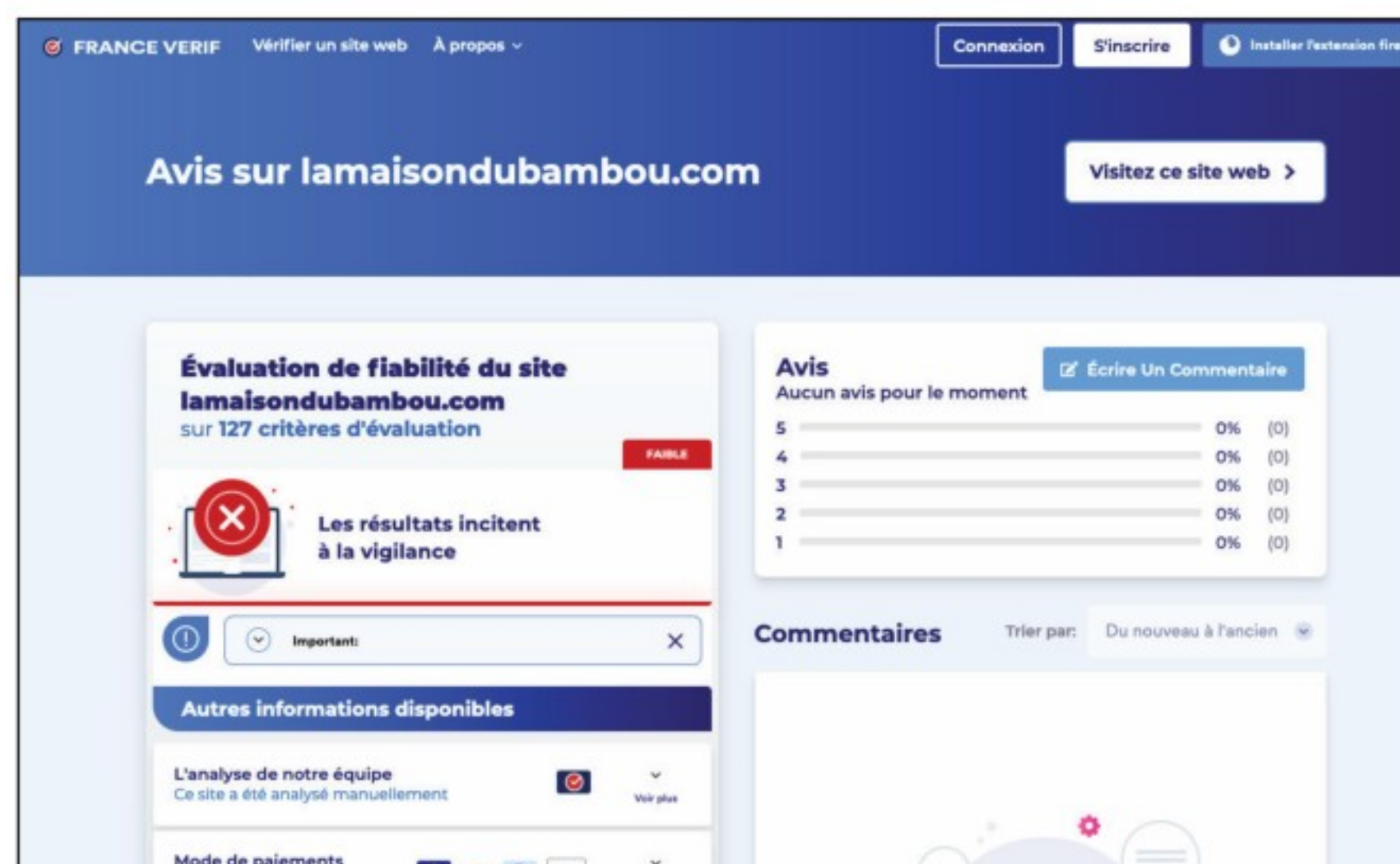
Lien : scamdoc.com/fr



FRANCE VERIF, POUR UNE VISION GLOBALE

France Verif analyse pour vous de nombreux éléments d'un site : adresse physique, mentions légales, technologies utilisées ou même popularité. Il s'appuie sur 127 critères d'évaluation différents, pour un regard assez complet. Petit bonus, il existe en extension sur la plupart des navigateurs !

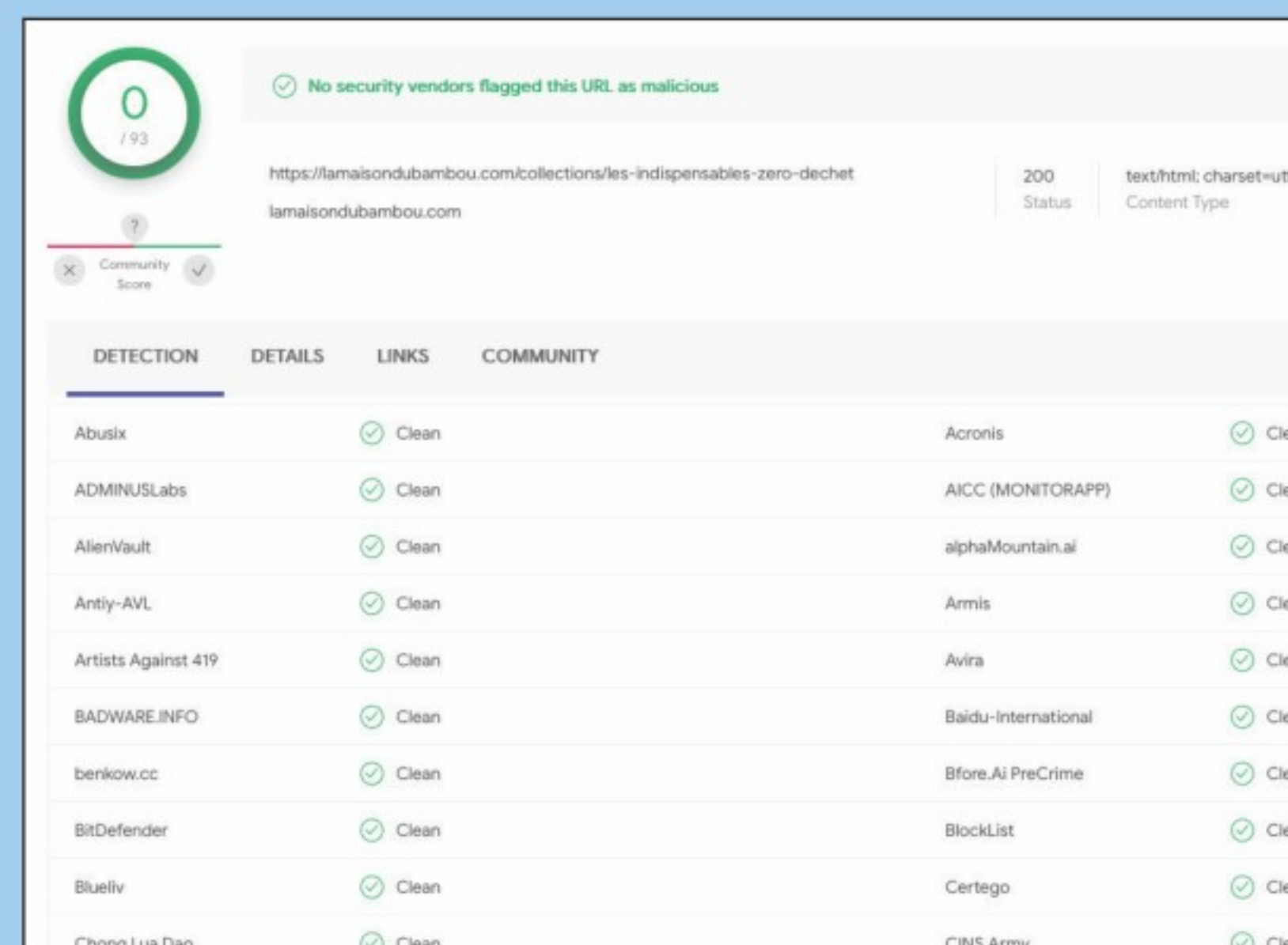
Lien : franceverif.fr



VIRUS TOTAL, POUR UNE ANALYSE CROISÉE

La plupart des antimalwares proposent une analyse et des alertes en temps réel lorsque vous visitez des sites Web exotiques contenant des codes malveillants. Mais vous ne pouvez jamais être certain que votre antivirus possède toutes les bases de signatures et de signalements à jour. En cas de doute, pourquoi ne pas utiliser Virus Total, qui s'appuie sur l'analyse de dizaines de solutions de cybersécurité parmi les plus connues ou les plus spécialisées (phishing, spam, scam, etc.)! Parmi elles, vous trouverez notamment Kaspersky ou BitDefender, ce qui peut être assez rassurant. Pour ce faire, rendez-vous sur l'onglet URL de Virus Total et lancez l'analyse du site sur lequel vous avez un doute.

Lien : virustotal.com





POUR QUI ?

Pour ceux qui acceptent qu'un PC ne soit pas éternel

POUR QUOI FAIRE ?

Protégez vos données de façon automatisée et fiable

SAUVEGARDEZ vos FICHIERS SANS Y PENSER AVEC FBackup



Qui n'a jamais perdu des heures de travail parce que son ordinateur a planté ? Les disques durs externes, le cloud et tout ça, c'est très bien. Mais c'est encore mieux si vous n'avez même plus besoin de réfléchir pour les utiliser.

Un ordinateur vous fait gagner un temps précieux... à condition que vous n'ayez pas oublié d'effectuer une sauvegarde juste avant que votre disque dur ne se crashe en beauté. Dans ce genre de circonstances, même Gollum ne peut plus rien pour vous. Sauf si vous

connaissiez un Gollum informaticien chevronné, capable de fouiller les miettes de vos composants pour vérifier s'il retrouve quelques données utiles. Or, tout le monde le sait : Gollum n'est pas toujours fiable et il coûte cher. Pour retrouver votre précieux travail, il vaut mieux s'appuyer sur une autre solution.

Et celle-ci n'a rien de magique : il s'agit de la sauvegarde automatique.

EFFICACITÉ GARANTIE

Le principe est simple : vous utilisez un logiciel qui sauvegarde automatiquement vos données. Toutes vos données. Et qui les envoie sur un support externe où vous n'aurez plus qu'à aller les récupérer en cas de besoin. Pas besoin de faire trois tomes avec cette histoire : même sa mise en route se programme en quelques clics !

VOUS ÊTES LE MAÎTRE À BORD

En la matière, FBackup est pratique et assez complet. Avec ses nombreuses fonctionnalités et options, il peut effectuer beaucoup de choses pour vous. Mais il ne fera pas tout non plus. Si vous ne prenez pas le temps de le configurer selon vos besoins, et notamment si vous vous contentez des sauvegardes manuelles... et que vous oubliez de les activer, il vous sera aussi inutile qu'une ceinture antigravité dans l'espace. Vous perdrez tout et vous n'aurez plus rien à quoi vous rattacher.

MÊME POUR LES FICHIERS OUVERTS

L'un des intérêts de FBackup, c'est qu'il conserve une copie des documents sur lesquels vous êtes en train de travailler. Même si vous êtes en train de les utiliser au moment de la sauvegarde. Petit bonus intéressant : parmi les sources à sauvegarder, vous pouvez aussi sélectionner des éléments figurants sur votre cloud, sur lesquels vous avez effectué des modifications en ligne.

Autant d'options qui ajoutent encore un peu de sécurité à l'ensemble (c'est le mode ceinture de sécurité + airbag pour vos données).

À SAVOIR

PLUGINS ET ASSISTANTS

Parce qu'il n'y a pas que le travail dans la vie, FBackup propose aussi des plug-ins pour vous aider à sécuriser vos sauvegardes de jeu (ouf). Il comprend également des assistants pour vous guider lors de sa mise en route et pour les restaurations de fichier (malheureusement, ces derniers n'apportent pas le café).

Votre tâche principale est de configurer FBackup selon vos besoins. Ce dernier s'occupe ensuite de tout pour garantir votre sérénité.

LES QUATRE QUESTIONS À SE POSER



Avec FBackup, vous pouvez conserver l'ensemble des données de votre ordinateur (et pas seulement vos fichiers préférés). Pas de choix de Sophie à effectuer ni de réflexion du style « Est-ce que j'ai bien conservé la dernière version en cours de mon document ? ».

Vous n'avez que quatre questions à vous poser :

- OÙ ENVOYER LA SAUVEGARDE ?

Sur un disque dur externe ou sur le cloud, notamment Google Drive ou Dropbox (parce que conserver vos fichiers en double sur votre propre ordinateur n'aurait que peu d'intérêt).

- QU'ALLEZ-VOUS SAUVEGARDER ?

Avez-vous vraiment besoin de conserver tous les mails s'ils sont sur un serveur externe ? Voilà le genre de questions à vous poser.

- QUEL TYPE DE SAUVEGARDE ?

Pour limiter la place sur votre support, le logiciel peut automatiquement compresser vos fichiers... ou pas.

- QUAND FAIRE DES SAUVEGARDES ?

Vous pouvez la lancer manuellement ou la programmer pour ne plus avoir à y penser (ce qui vous assure quand même le maximum de tranquillité).





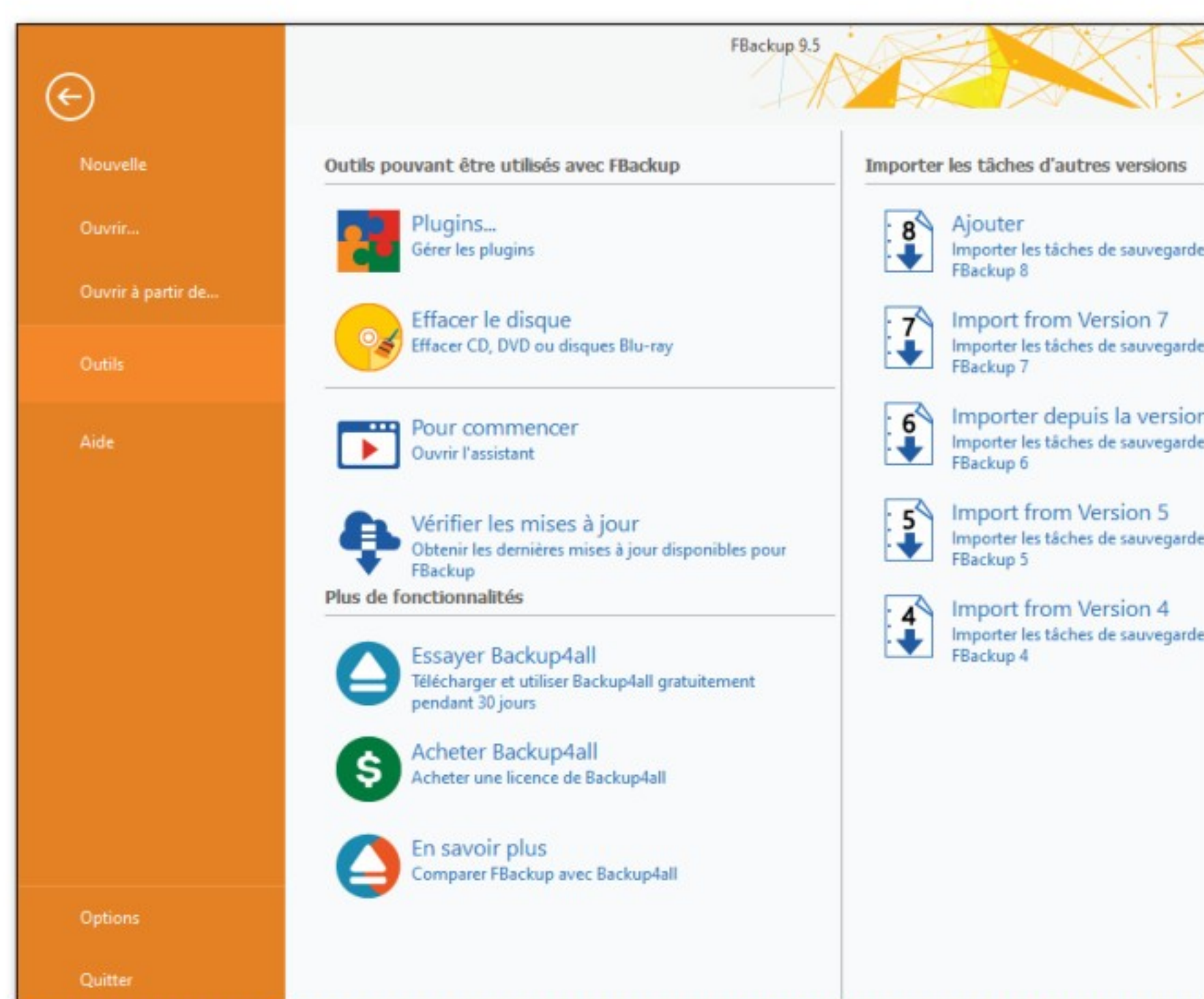
CONFIGUREZ VOS SAUVEGARDES



Votre principale mission, si vous l'acceptez, est de préparer la manière dont vos sauvegardes seront mises en place. Grâce à l'assistant intégré de FBackup, cela ne devrait pas vous poser de problème.

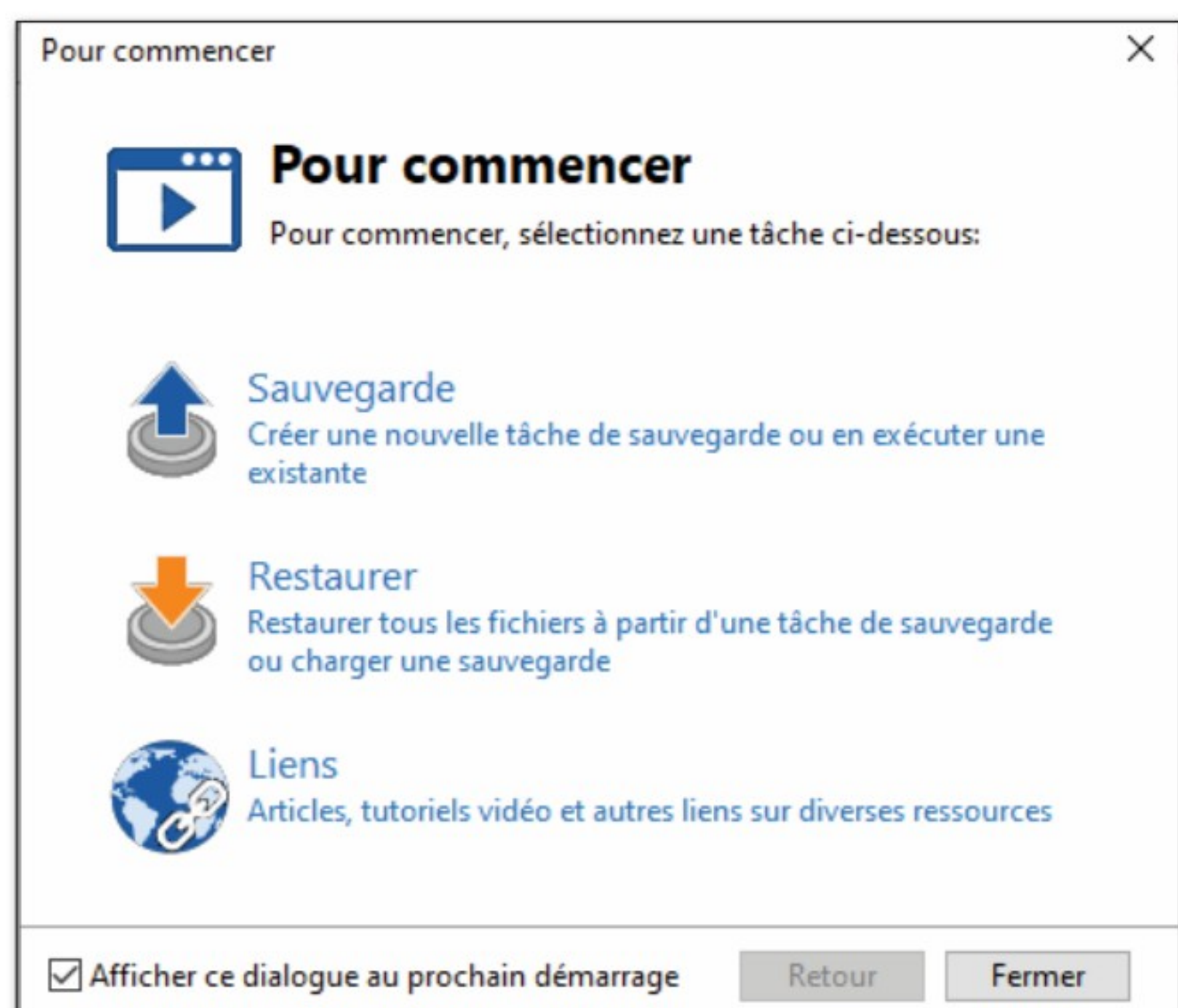
01 > ACCÉDER À L'ASSISTANT

Une fois le programme installé, cliquez sur **Fichier**. Vous ouvrirez ainsi un menu général qui vous donne accès à l'ensemble des fonctions de base. Cliquez alors sur **Pour commencer** pour ouvrir l'assistant.



02 > DÉCIDER D'UNE ACTION

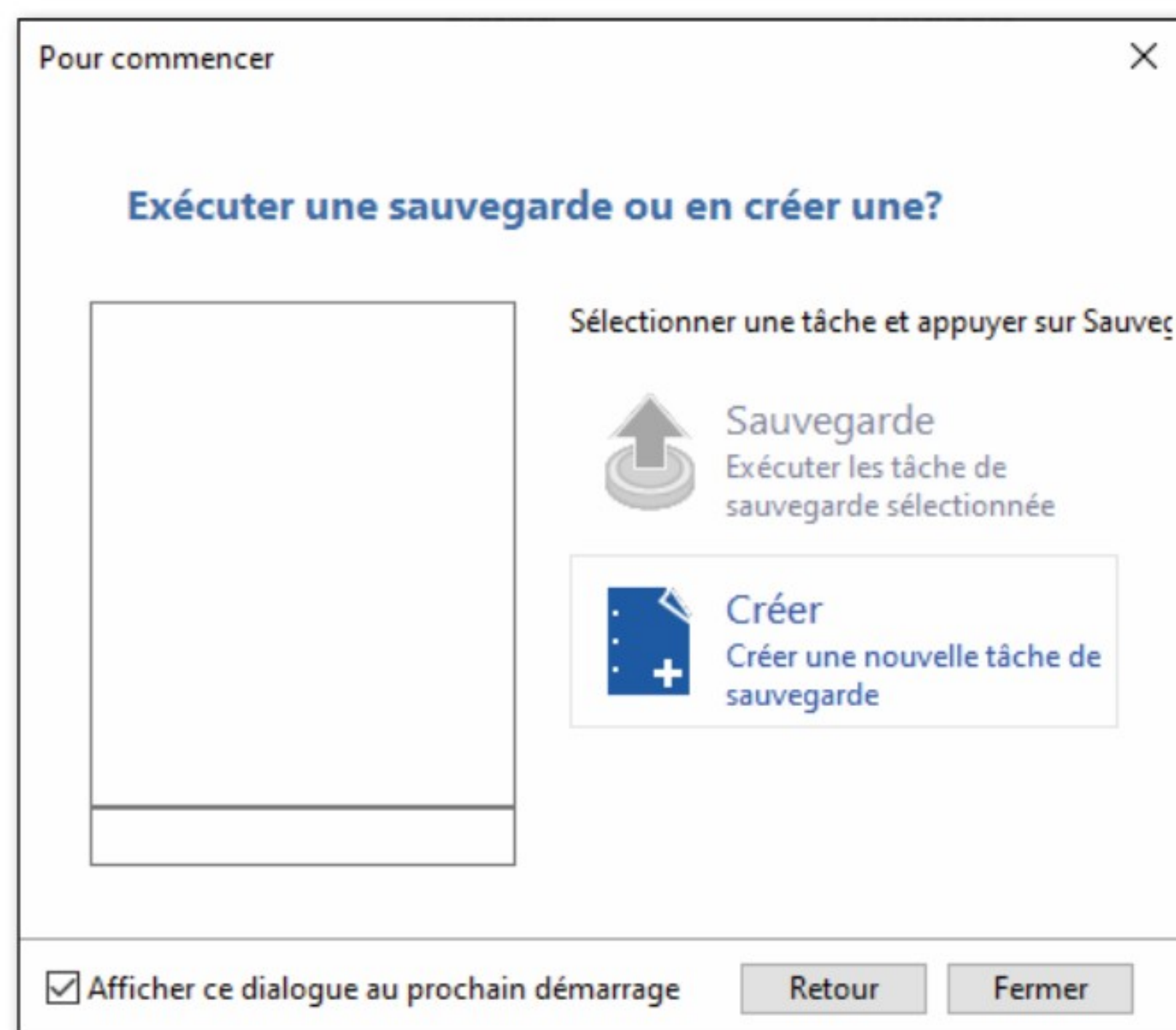
Quand l'assistant est ouvert, vous pouvez créer une nouvelle sauvegarde (**Sauvegarde**) ou charger une



sauvegarde antérieure (**Restaurer**). Pour votre première opération, cliquez sur **Sauvegarde** afin de programmer les actions à venir.

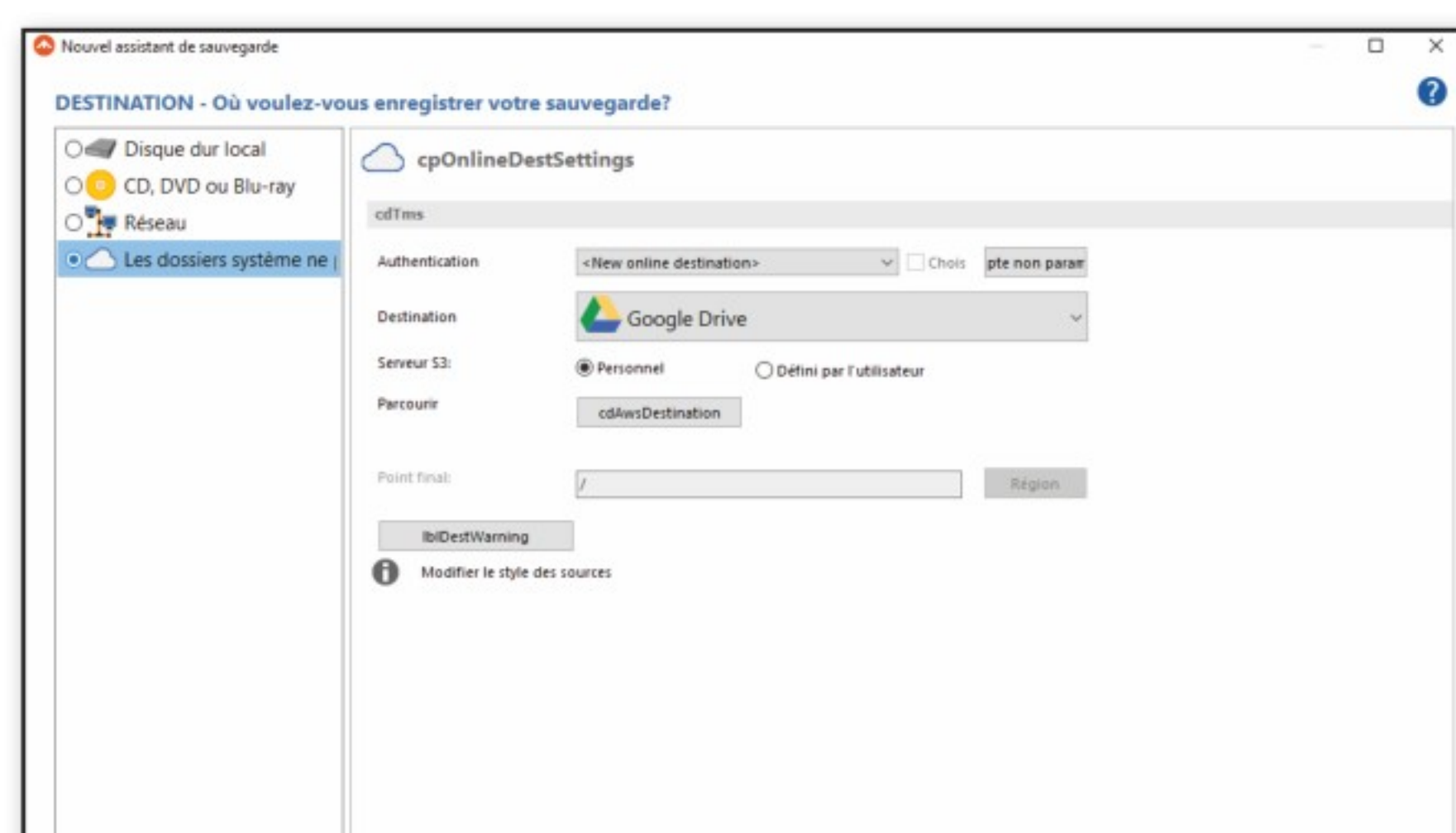
03 > CRÉER UNE SAUVEGARDE

FBackup tient à s'assurer qu'il effectue exactement ce dont vous avez besoin. Dans cet esprit, à ce niveau de votre activité, il vous demandera si vous voulez exécuter une sauvegarde déjà prévue ou **Créer** une sauvegarde. En théorie, seule cette icône sera cliquable à ce stade. Si vous ne l'avez pas fait précédemment, vous pouvez aussi décocher la case pour que ce menu ne s'affiche plus sauf demande expresse de votre part.



04 > CHOISIR UNE DESTINATION

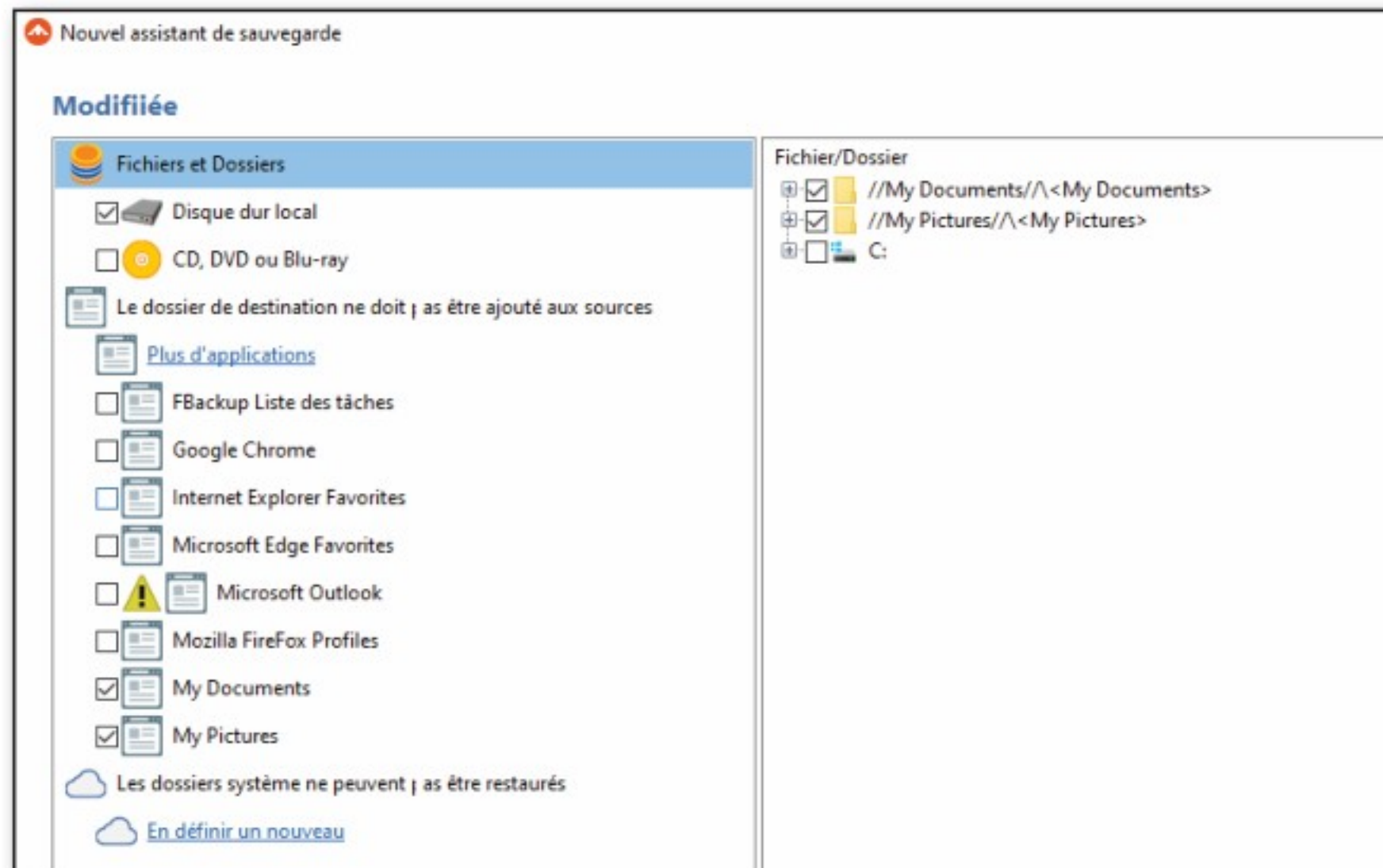
C'est là que cela devient intéressant : vous allez déterminer où les sauvegardes seront envoyées. Vous pouvez les conserver sur un disque dur, un support physique, le réseau ou dans le cloud. Pour sélectionner votre dossier Google Drive ou Dropbox (les deux seules options gratuites), cliquez dans la fenêtre juste après **Parcourir** et entrez les coordonnées de votre serveur de cloud.





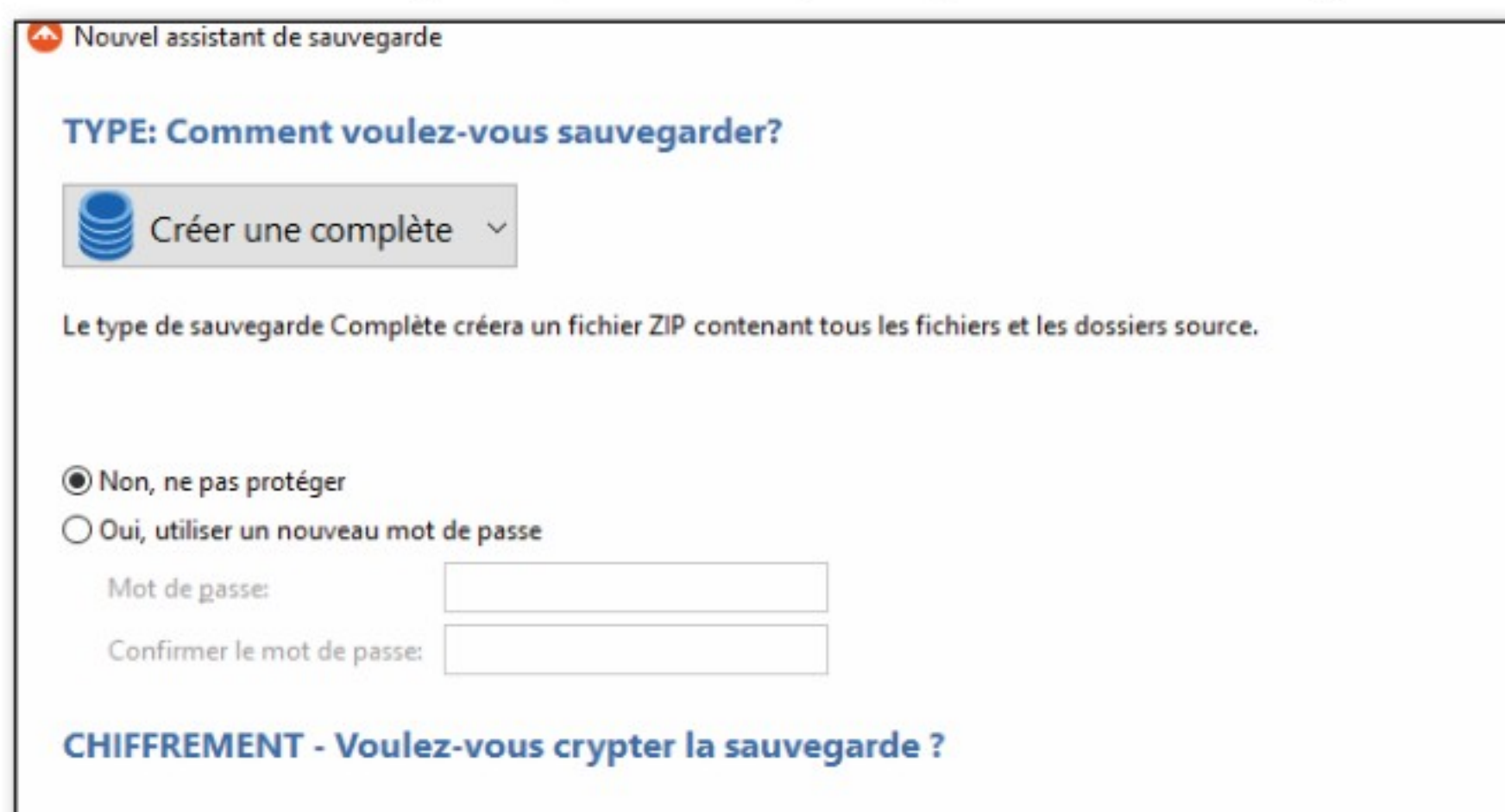
05 > SÉLECTIONNER DES DOSSIERS

Vous pouvez sélectionner les dossiers à sauvegarder soit via la fenêtre de l'assistant, soit en **Mode avancé** en les recherchant dans l'explorateur de fichiers, pour être encore plus précis. En mode classique, l'assistant vous proposera l'accès aux dossiers **Documents**, **Images** et aux favoris de vos navigateurs



06 > COMPRESSER OU NON

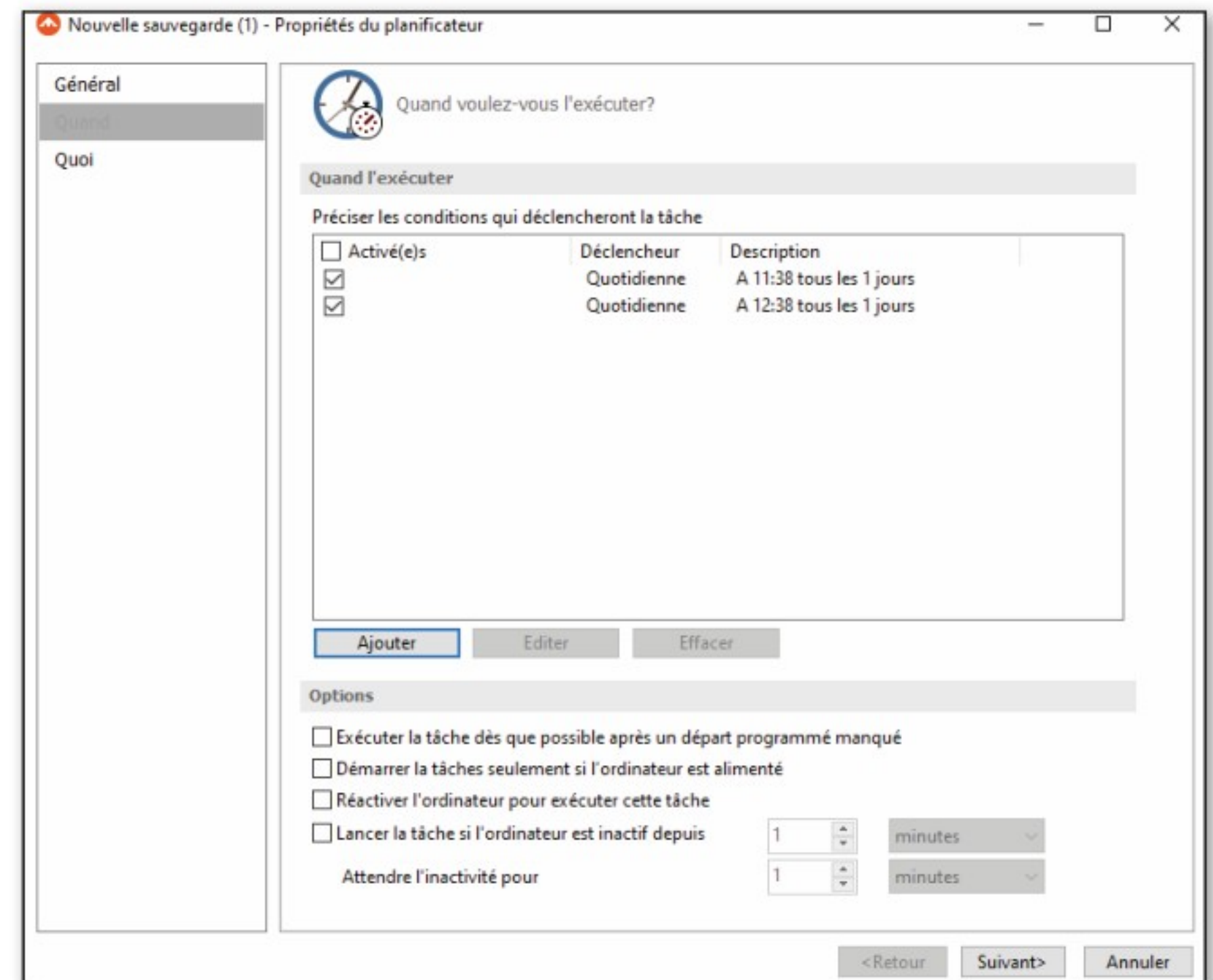
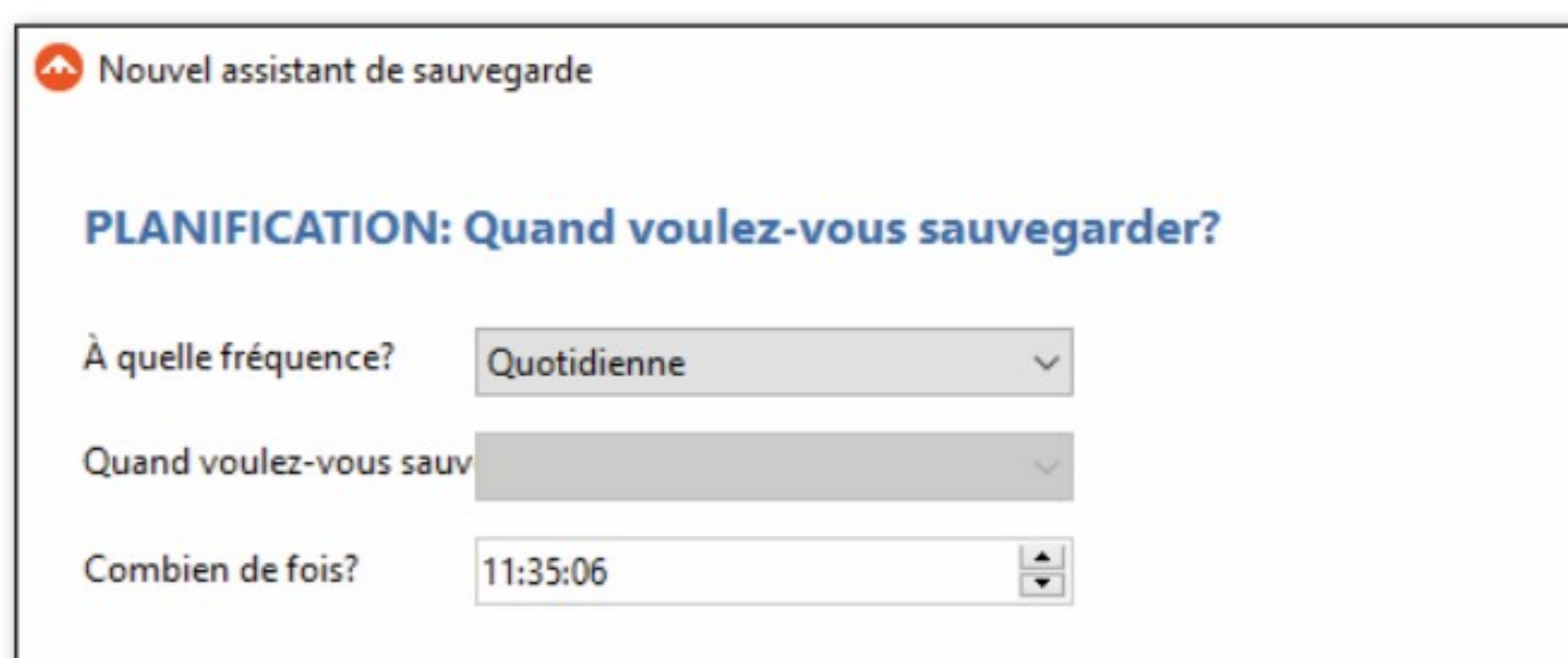
Vous pourrez ensuite décider de compresser les fichiers ou de les copier en mode miroir. Vous aurez aussi le choix de les protéger avec un mot de passe le cas échéant. Cette option peut être pratique si vous craignez de



perdre un jour votre support externe ou les piratages lors d'une sauvegarde sur le cloud, par exemple.

07 > PRÉVOIR LES SAUVEGARDES AUTOMATIQUES

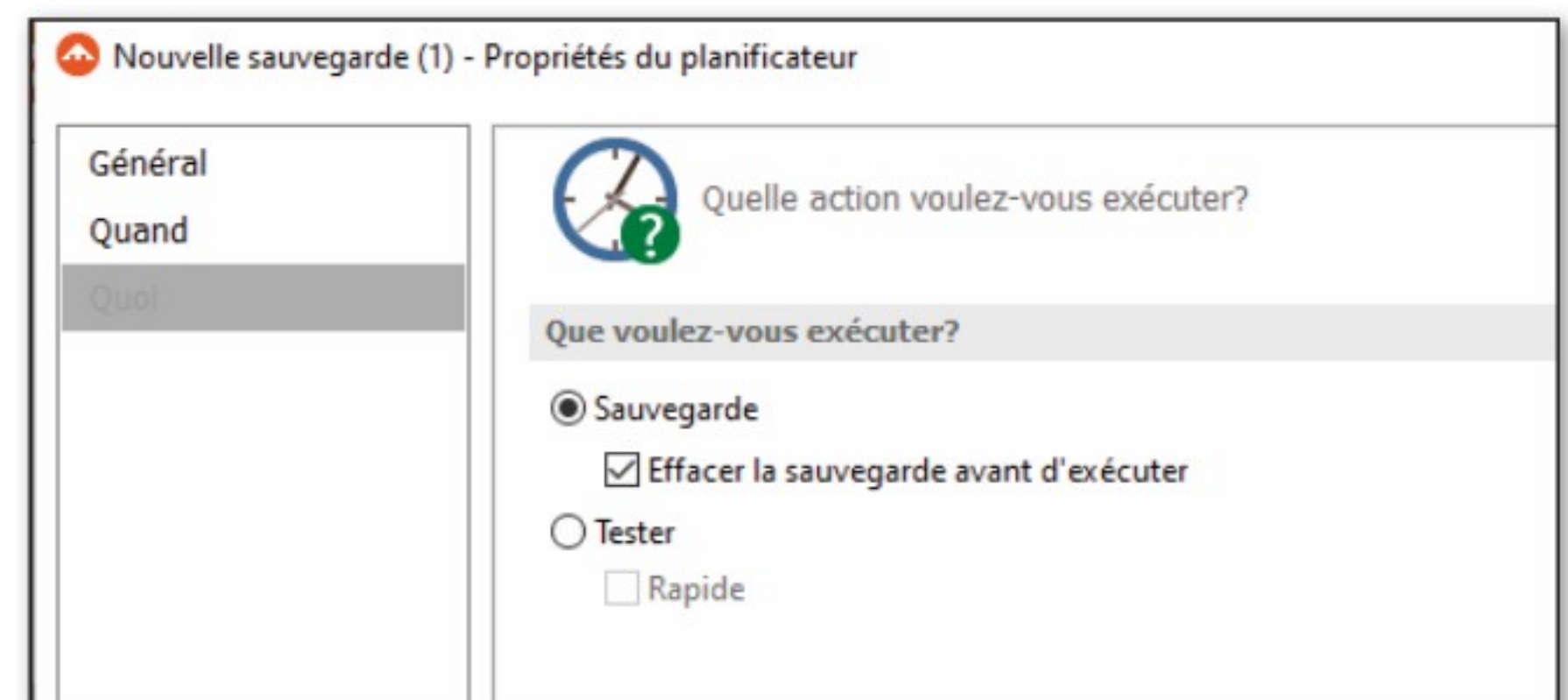
La fenêtre suivante vous permet d'accéder à la planification. Vous pouvez choisir la **Fréquence** (quotidienne, hebdomadaire, mensuelle). Si vous avez



besoin d'options supplémentaires, passez en **Mode avancé**. Là, vous ouvrirez le planificateur, ce qui vous permettra d'ajouter des dates et horaires (par exemple plusieurs fois par jour).

08 > GAGNER DE LA PLACE

Pour occuper moins d'espace disque, vous pouvez (toujours en mode avancé), décider d'**Effacer la sauvegarde avant de l'exécuter**. Ainsi, les éléments précédents seront



automatiquement supprimés (à ne cocher que si vous êtes sûr de ne plus devoir y accéder).

À SAVOIR

En théorie, FBackup devrait se configurer automatiquement selon les paramètres de votre ordinateur. Néanmoins, si vous avez besoin de modifier la langue, allez dans les **Options** du menu **Fichier**. Ce sera l'un des principaux critères sur lesquels vous pourrez agir. Et sans doute l'un des plus pratiques pour vous y retrouver dans les différentes options. Par ailleurs, vous retrouverez en ligne de nombreux tutoriels pour vous guider. Et ils sont même accessibles depuis l'assistant présenté sur la page précédente !



PROTECTION



AJOUTEZ DES FONCTIONS SUPPLÉMENTAIRES

PRATIQUE



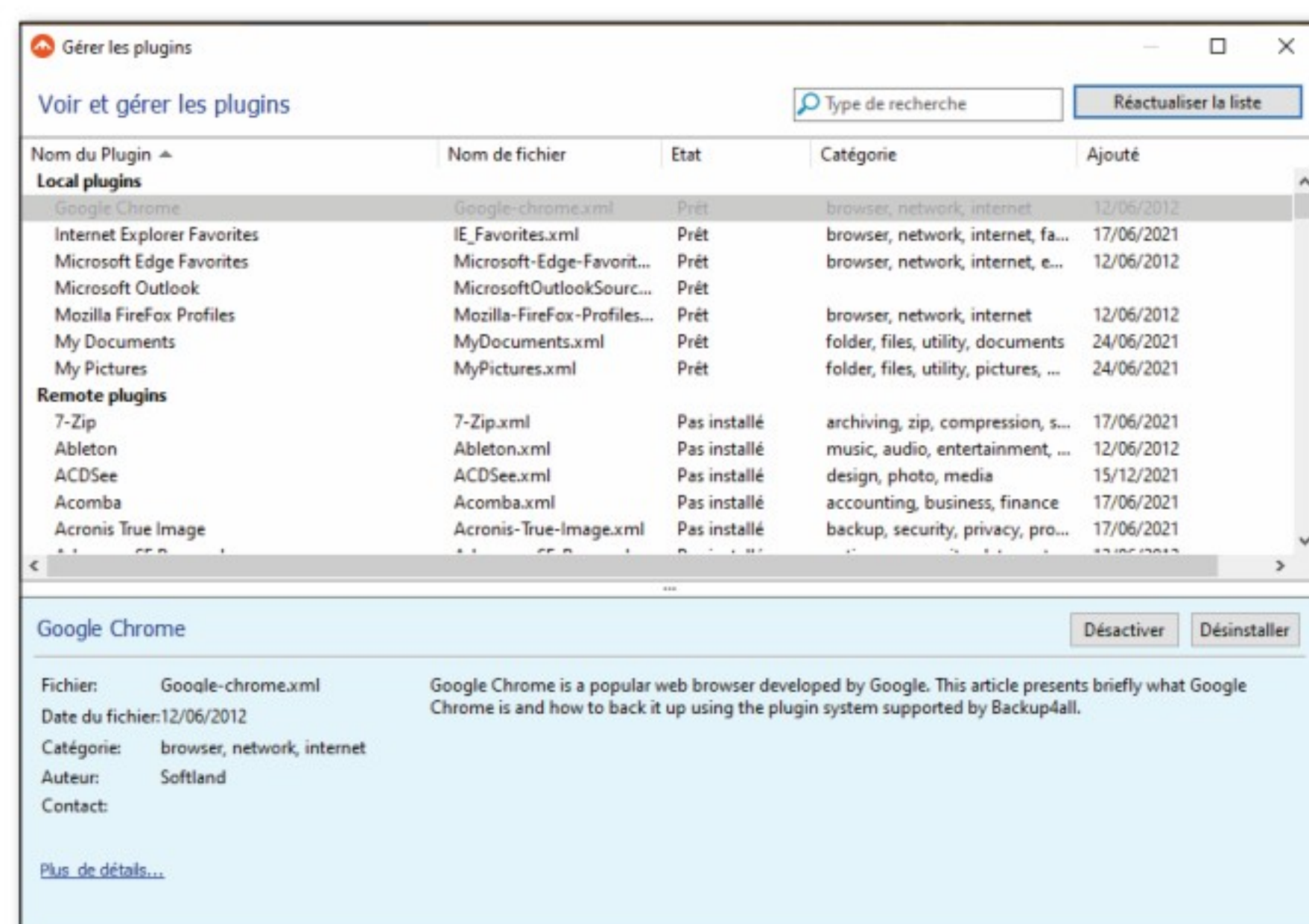
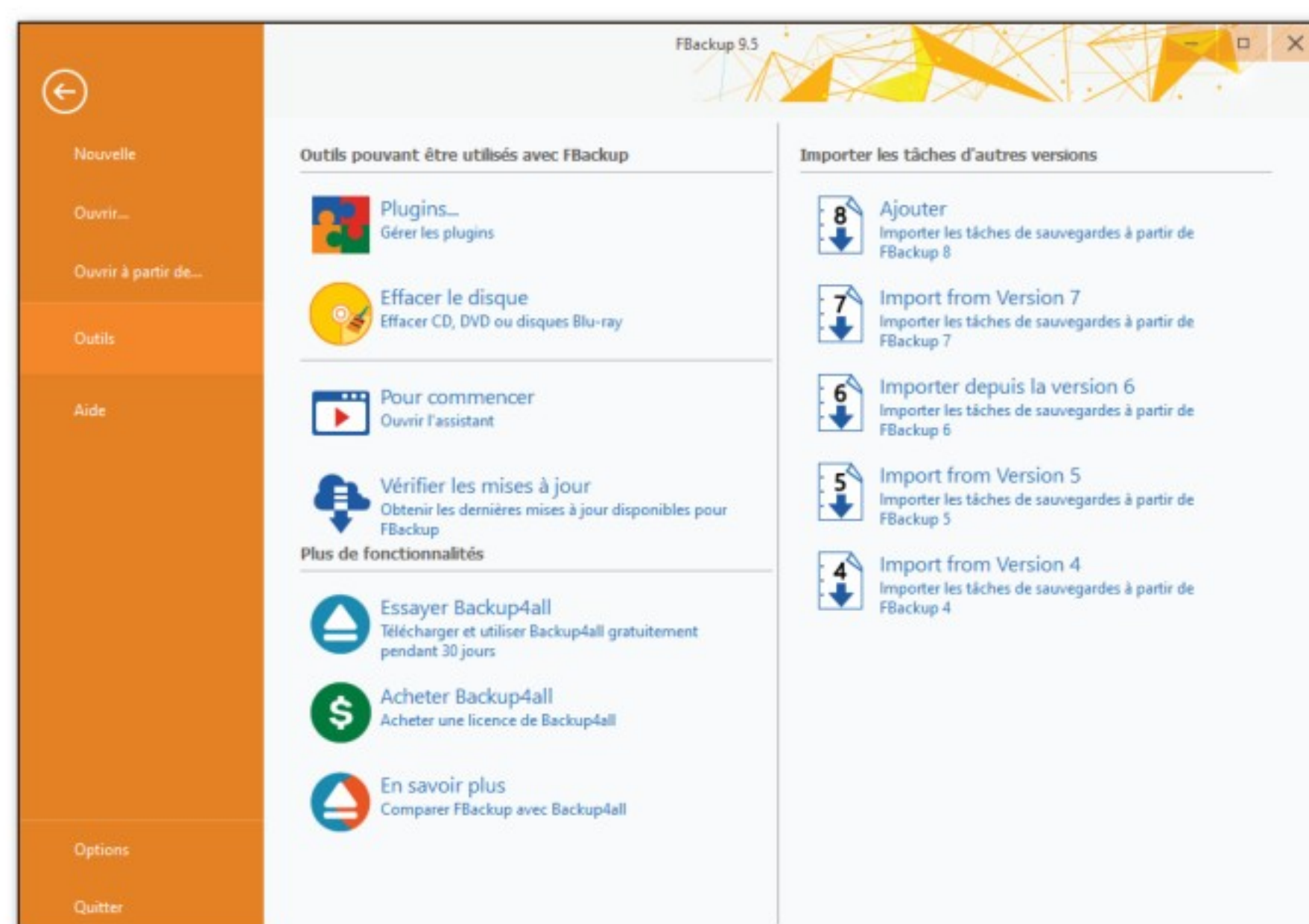
Fbackup s'adapte à vos besoins. Si vous avez besoin de conserver précieusement vos sauvegardes de jeu ou de téléchargements divers, il saura aussi le faire pour vous grâce aux plug-ins dédiés.

01 > ACCÉDER AUX PLUG-INS

Depuis le menu **Fichier**, cliquez sur **Plug-ins**. Vous accéderez ainsi à une liste complète de tous les plug-ins existants pour l'application. Ils sont déjà nombreux mais vous pouvez aussi en suggérer d'autres si votre programme préféré n'en fait pas encore partie.

02 > INSTALLER UN PLUG-IN

Les plug-ins déjà présents seront indiqués en haut de la liste. Tous les suivants se trouvent sous l'indication **Remote plug-ins**. Faites défiler, ils sont classés en fonction des noms des logiciels auxquels ils se réfèrent. Il ne vous reste plus qu'à les installer



ACCÉDEZ À VOS SAUVEGARDES

PRATIQUE



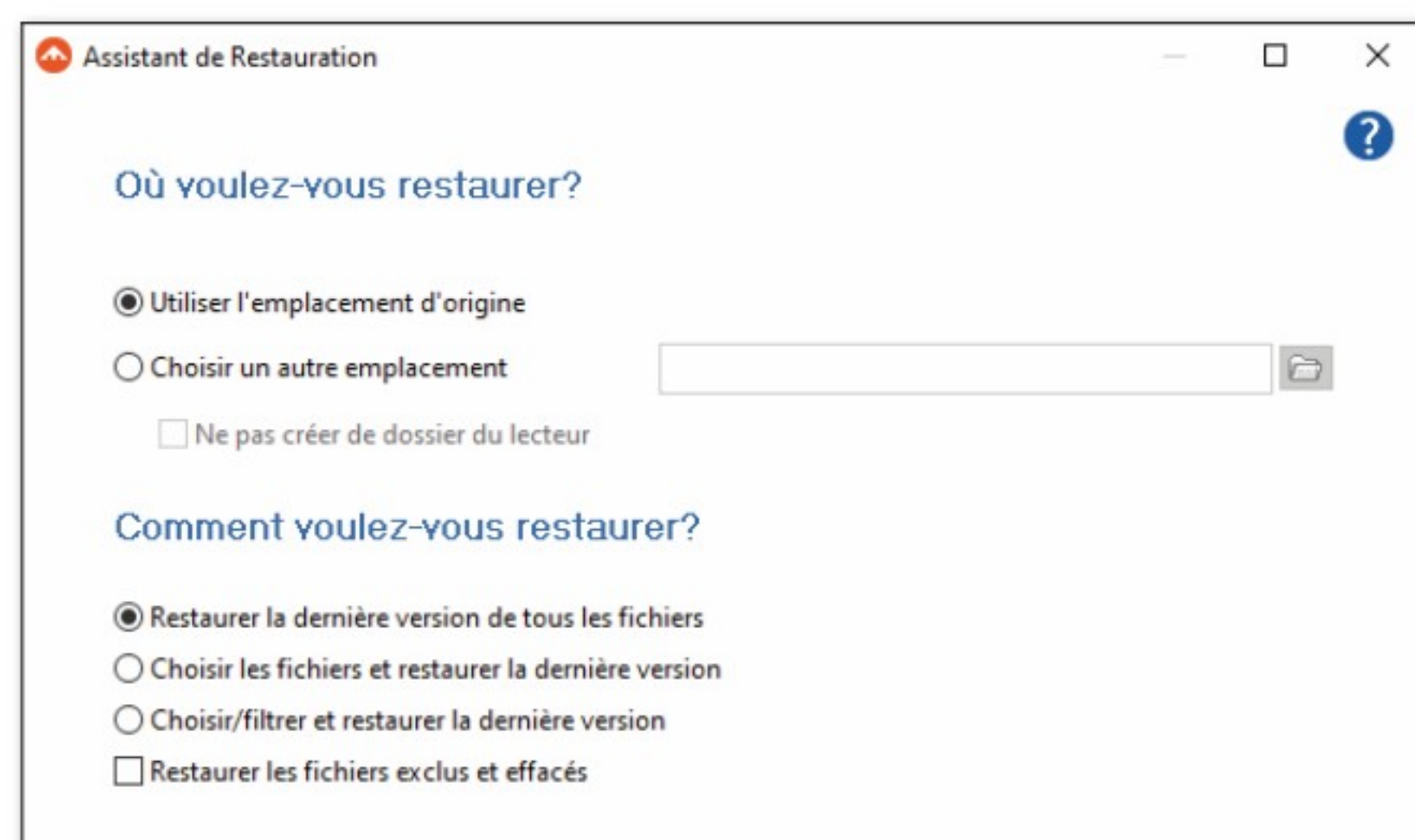
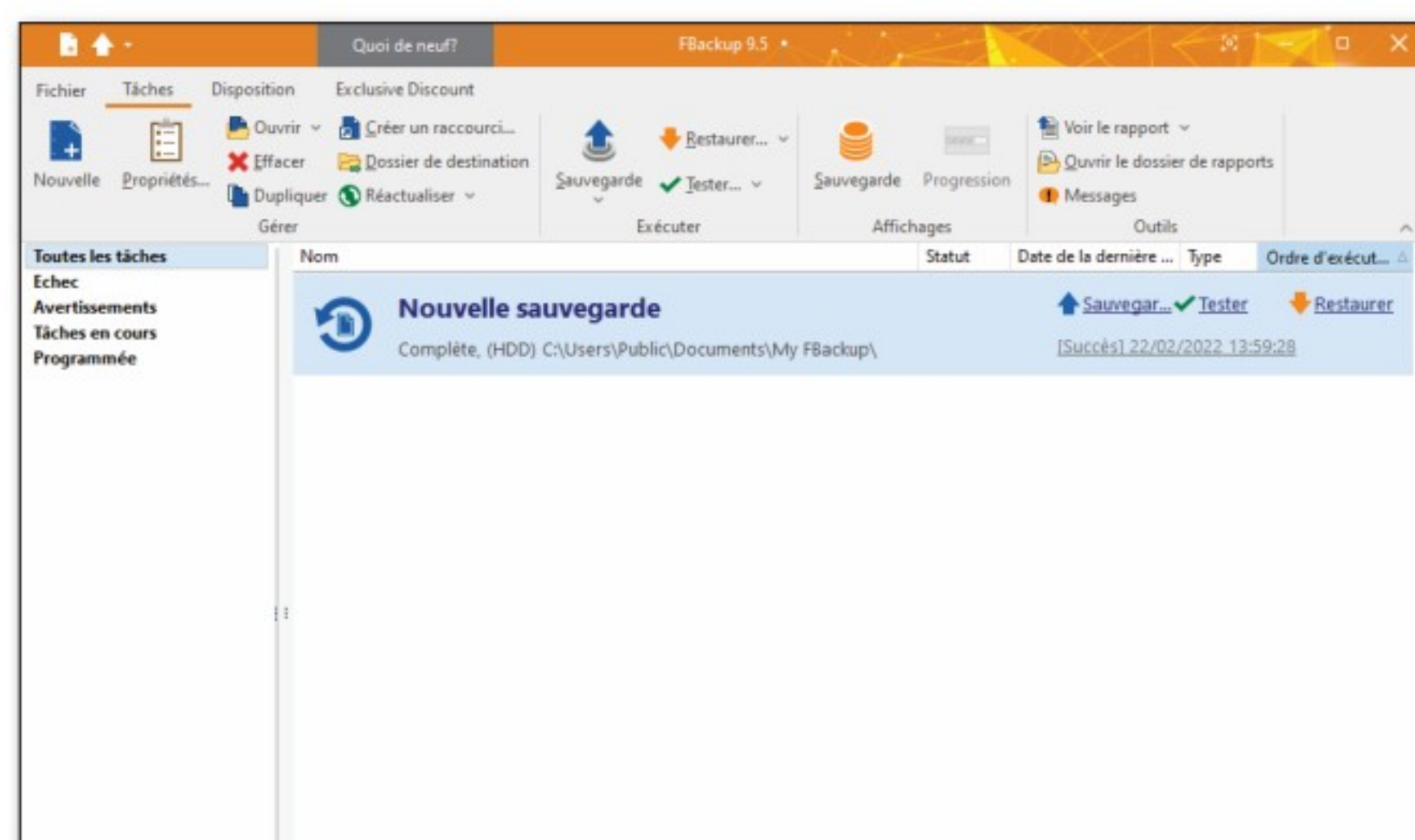
Vous ne vous rappelez plus où vos sauvegardes sont enregistrées ? Pas de souci, il vous suffit de les restaurer.

01 > ACCÉDER À LA RESTAURATION

Aller sur le menu **Tâches**. Les sauvegardes effectuées apparaissent dans l'ordre chronologique. Cliquez sur **Restaurer** pour accéder à l'assistant de restauration.

02 > SÉLECTIONNEZ LES OPTIONS

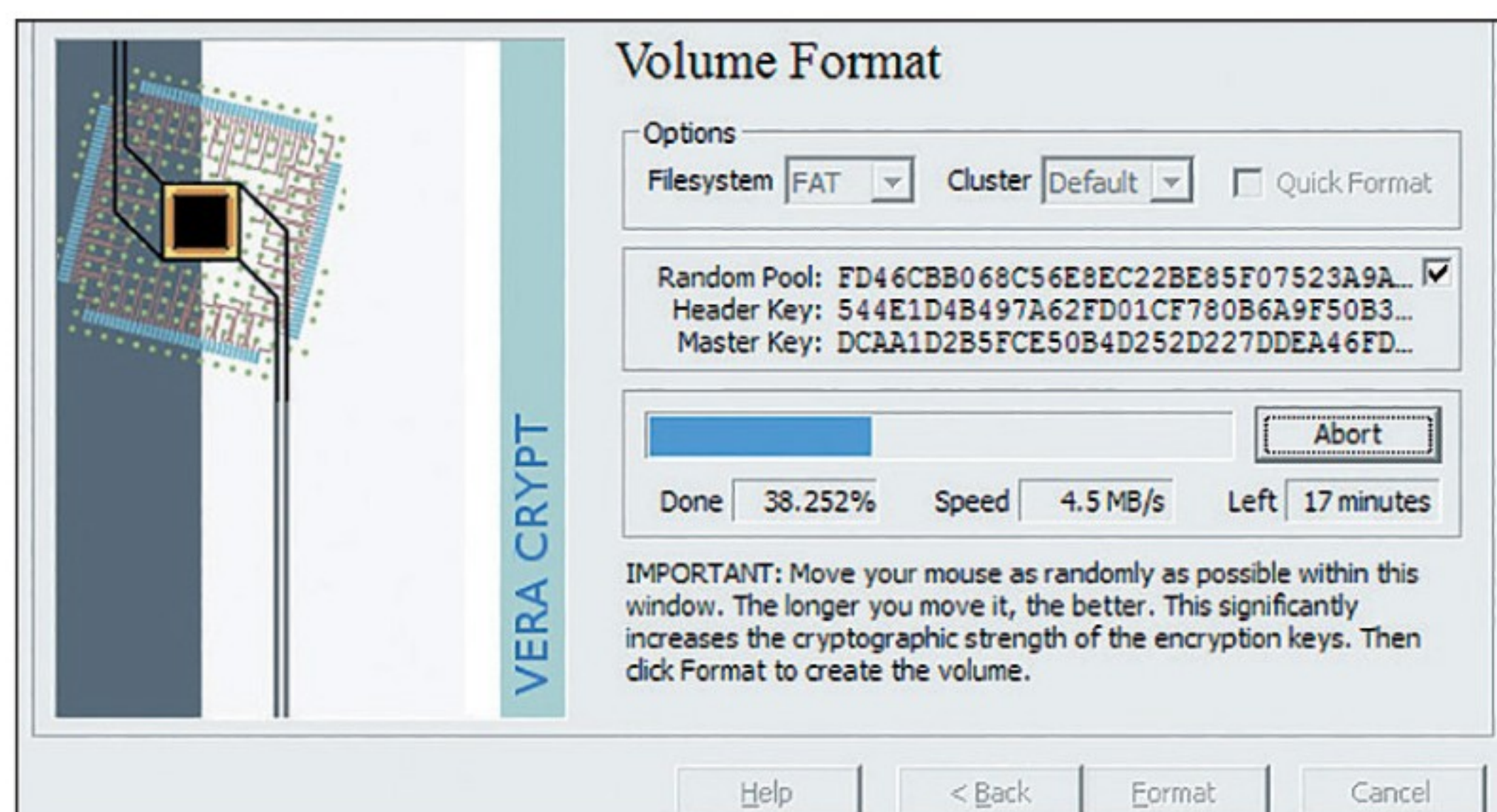
Comme pour toutes les autres fonctions, Fbackup vous laisse le choix. Vous pouvez restaurer vos fichiers dans leur emplacement d'origine et choisir uniquement ceux dont vous avez besoin (en cliquant sur **Choisir les fichiers et restaurer la dernière version**).



Chiffrer un disque ou une clé USB > AVEC VERA CRYPT

Chiffrer les données d'un disque dur vous permet de vous assurer de la confidentialité de ces données, même dans le cas où un attaquant a un accès physique au disque dur, par exemple dans le cas d'un vol d'ordinateur portable. Pour cela, vous pouvez utiliser VeraCrypt, un logiciel open source et gratuit de chiffrement de données. VeraCrypt permet de chiffrer et déchiffrer les données à la volée, c'est-à-dire de manière transparente pour l'utilisateur et le système. Il est possible de créer un volume chiffré sur un disque dur, une partition ou une clé USB.

Lien : www.veracrypt.fr

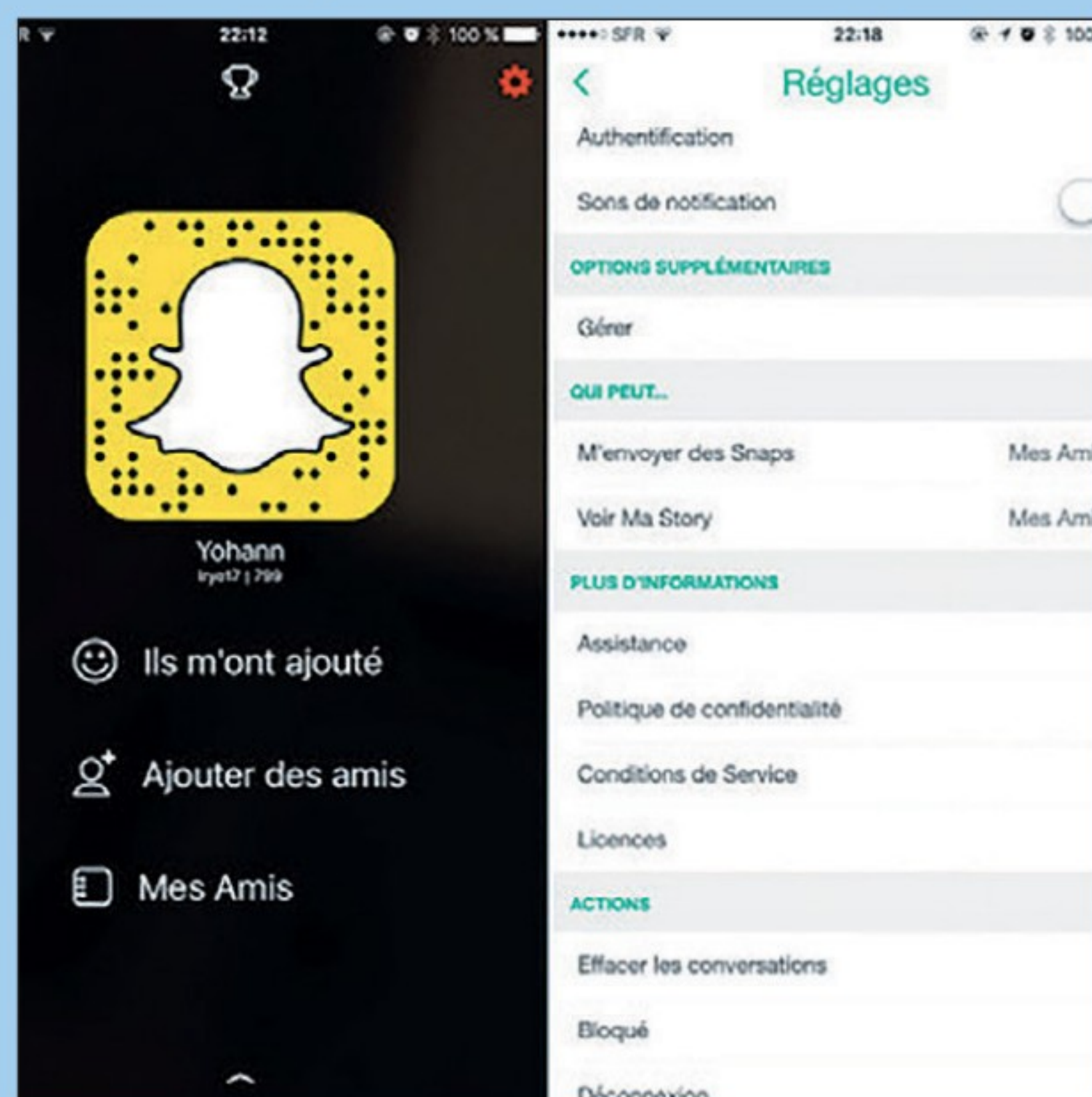


Masquer son identité

> AVEC SNAPCHAT

Snapchat n'est pas sans risque. Pour éviter les surprises, il faudra passer par les réglages... Commençons par masquer votre numéro de téléphone pour éviter d'être enregistré par des utilisateurs que vous ne connaissez pas ou que vous ne souhaitez pas connaître. Allez dans les **Paramètres généraux** puis décochez la case **Autoriser mes amis à me retrouver**. Au même endroit vous trouverez **Qui peut m'envoyer des Snaps** puis **Mes amis**. Vous réduirez les risques de vous faire importuner. Dernière précaution : utilisez un pseudo. Celui-ci protège votre identité ou vous permet d'être introuvable à partir de votre nom / prénom !

Lien : www.snapchat.com

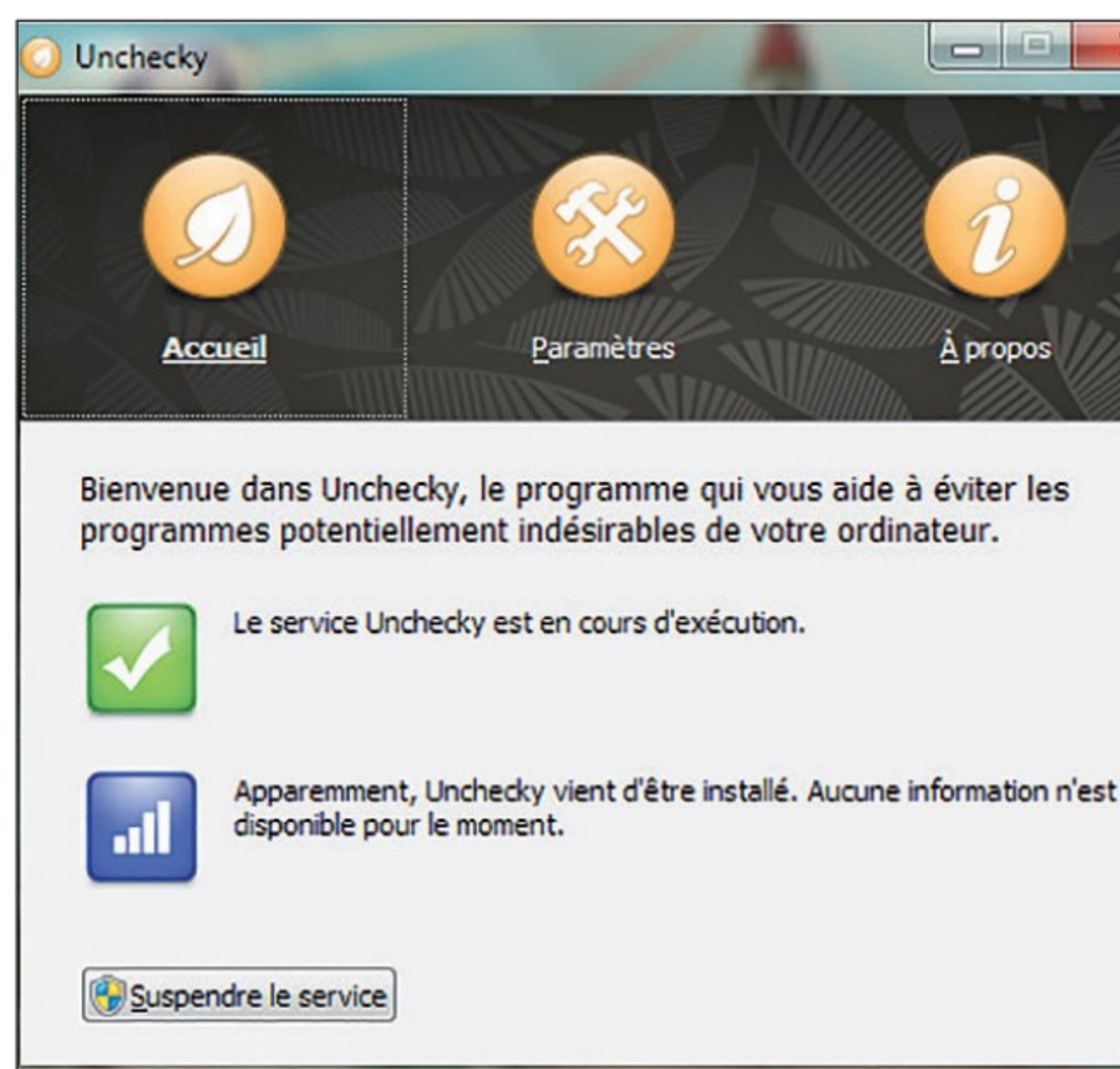


Finissez-en avec les barres d'outils et les adwares

> AVEC UNCHECKY

Si vous avez la sale habitude d'installer des logiciels en permanence pour les tester, vous devez avoir un navigateur aussi chargé en barre d'outils et en adwares qu'un stagiaire de la rédaction. En effet, certains logiciels vous installent automatiquement des saletés à moins qu'il ne s'agisse d'une erreur de manipulation de votre part. Pour éradiquer ces programmes, parfois introuvables dans le module de désinstallation du panneau de configuration, il existe Browser Cleaner, mais pourquoi ne pas traiter le mal à la base ? Le logiciel Unchecky va tout simplement «décocher» les cases fautives. Vous n'aurez plus à lire avec attention les fenêtres qui s'afficheront lors d'une prochaine installation.

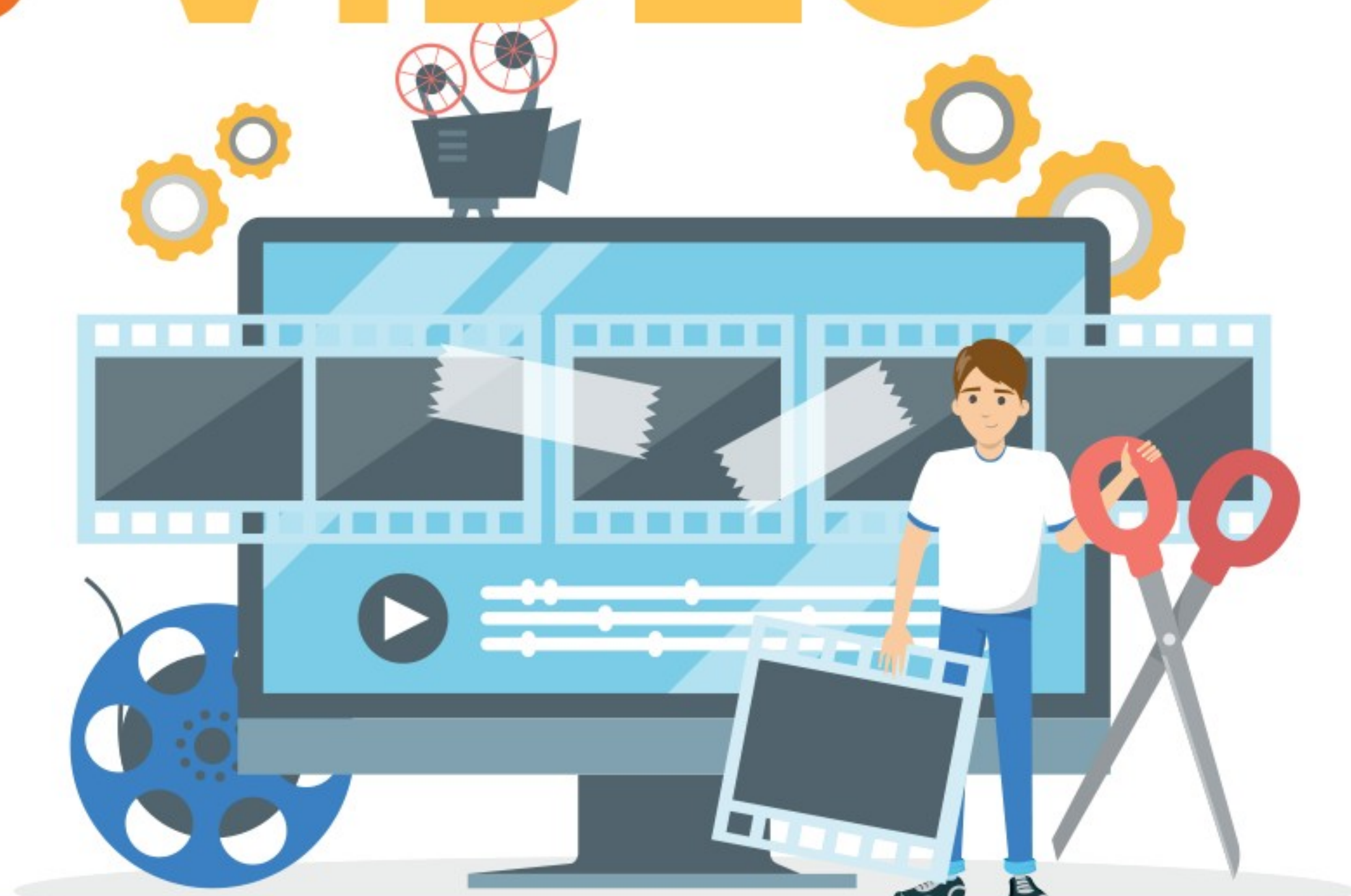
Lien : <https://unchecky.com>





TOP 5 MONTAGE VIDÉO

Certains logiciels utilisés par Hollywood sont maintenant accessibles gratuitement. Allez plus loin qu'avec Windows Movie Maker et prenez-vous pour le prochain Spielberg. Vous pouvez même utiliser un smartphone pour tourner, comme Steven Soderbergh...



DAVINCI RESOLVE > LE PLUS PRO

Ce logiciel, conçu par les fabricants de caméras professionnelles Black Magic, est utilisé au cinéma. Des films récents, comme *Red Notice*, ont été étalonnés avec lui. Son interface est cependant meilleure que ce long métrage et se révèle particulièrement intuitive. Même si vous débutez dans le monde du cinéma, vous la prendrez en main sans aucun souci. S'il est surtout reconnu pour la puissance de sa fonction de correction colorimétrique, DaVinci Resolve inclut de nombreuses fonctions. Certaines peuvent sembler abruptes pour les amateurs, mais un petit didacticiel de démarrage vous accompagnera lors de la prise en main. Par la suite, vous aurez accès à plusieurs centaines de sons et de bruitages libres de droits. Par contre, DaVinci Resolve nécessite beaucoup de Ram pour fonctionner, un (petit) détail à prendre en compte, surtout si votre ordinateur n'est pas des plus récents.

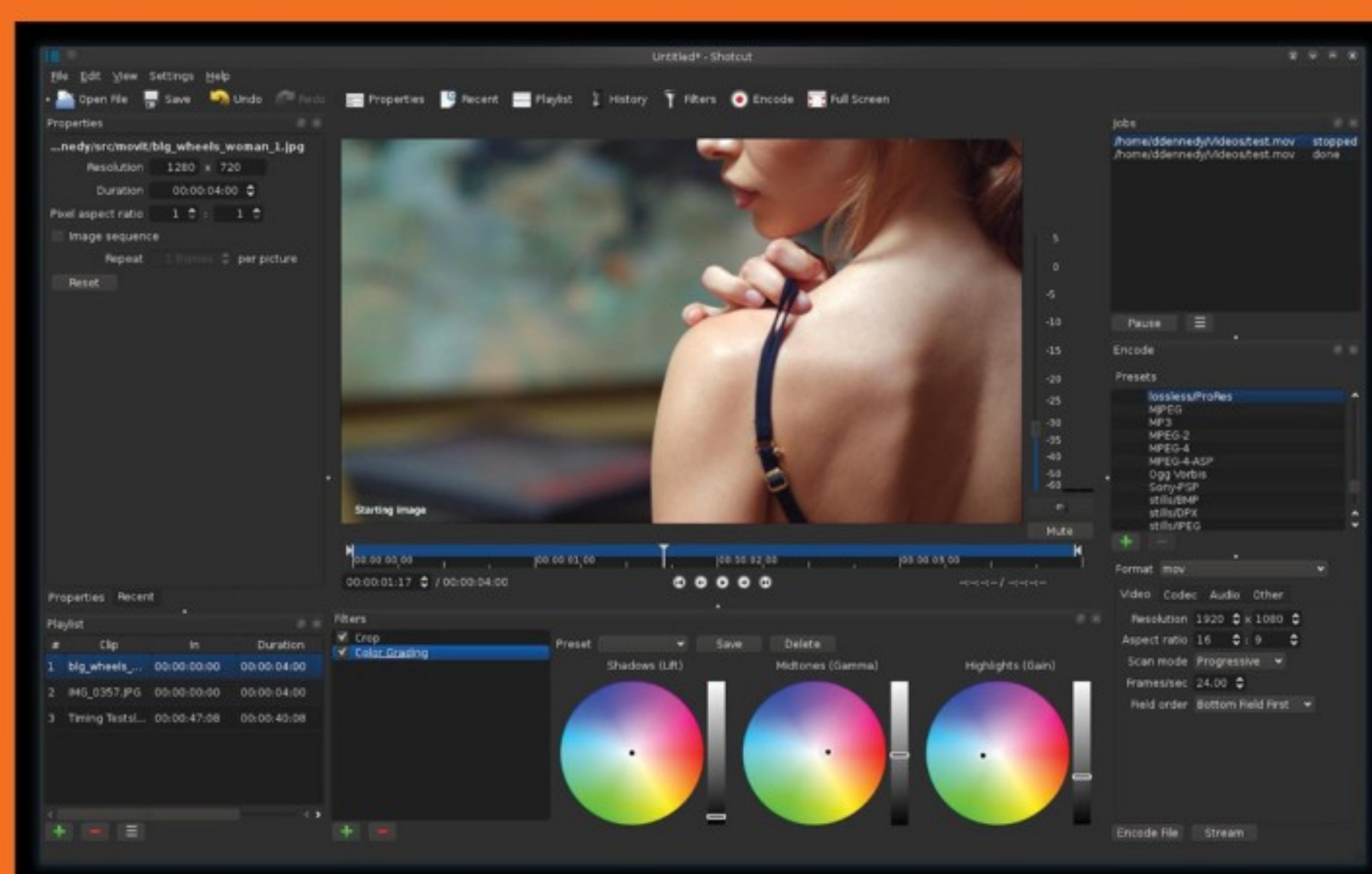
Lien : <https://bit.ly/3spjSQg>



Shotcut > L'OPEN SOURCE

Avec Shotcut, pas de fonctions payantes à ajouter. Quand vous le téléchargez, vous avez accès à tout. Ce qui ne signifie pas pour autant qu'il est facile à prendre en main. Son interface est particulière, sans doute parce qu'il a été d'abord conçu pour Linux, avant d'être adapté pour les environnements Windows. Pas de panique cependant : il est très populaire et vous trouverez en ligne de nombreux tutoriels pour découvrir ses fonctions. La plus appréciable : son large choix de filtres, aussi bien pour l'audio que pour le contenu vidéo. Ils peuvent même se superposer, pour des résultats encore plus uniques. Car ce logiciel se transforme selon vos besoins. Une fois téléchargé, il vous revient de le personnaliser. C'est vous qui décidez quels sont les modules nécessaires, et lesquels doivent s'afficher à l'écran. Par ailleurs, Shotcut inclut la résolution 4K HD (ce qui est rare parmi les logiciels gratuits), en plus d'une compatibilité avec tous les codecs audio et vidéo sur le marché.

Lien : shotcut.org



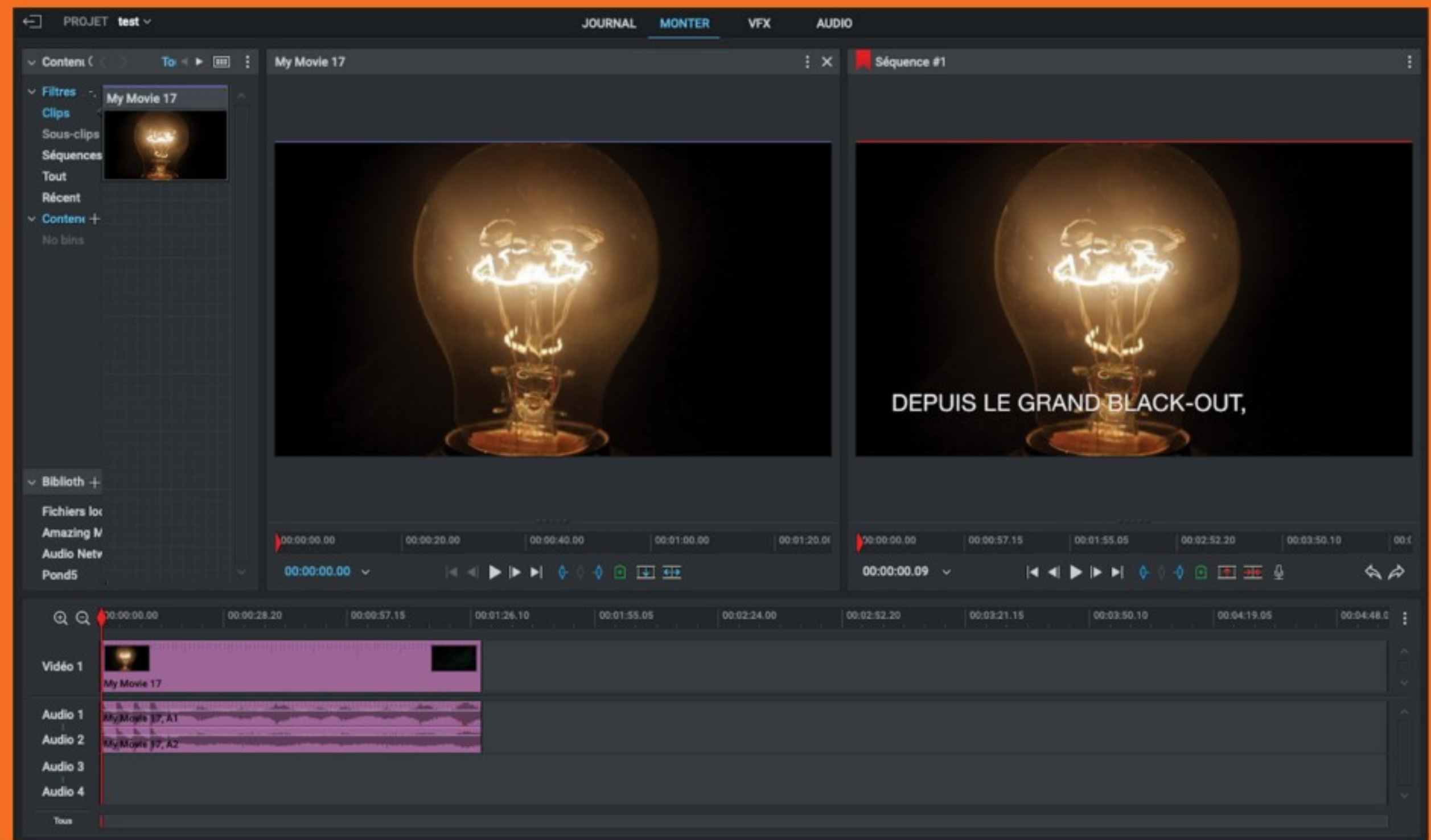


LIGHTWORKS > LE PLUS ANCIEN

Cet éditeur vidéo est sur le marché depuis 30 ans. Pendant cette période, il a permis de monter des films aussi connus que *Pulp Fiction* ou *Braveheart*. Par conséquent, son interface est peut-être plus dense à prendre en main pour les amateurs. Mais cela implique aussi un grand nombre de possibilités. Il est ainsi l'un des rares à prendre en charge les vidéos multipistes ou à permettre l'importation de séquences en arrière-plan. Ne vous inquiétez pas si le site vous propose un abonnement : il vous suffit de télécharger le logiciel et de vous

connecter tous les trois mois pour garder l'accès à la version gratuite. Autre avantage de taille : Lightworks se fait tout léger pour votre ordinateur. Par ailleurs, il prendra en charge tous les formats de vidéo. Hélas, dans sa version gratuite, la qualité de votre film ne pourra pas dépasser 720 p en sortie. Ce ne sera peut-être pas encore l'idéal pour le grand écran, mais ça devrait suffire pour une diffusion sur internet. À vous de savoir où se trouve votre public.

Lien : lwks.com



BLENDER > POUR LA 3D

Open source, Blender a d'abord été imaginé comme une suite d'animation 3D. Le montage vidéo est venu ensuite. Rassurez-vous : découpages et assemblages de séquences font bien sûr partie de son ADN, sans que le résultat ne soit une soupe insipide. Il permet le mixage audio et vous laissera jouer sur bon nombre de détails techniques, comme la forme d'onde de luminance ou les histogrammes. Avec lui, vous apprendrez aussi à compter jusqu'à 32 : il comporte 32 emplacements pour ajouter des vidéos, des images, de l'audio et des effets. Mais ce qui le différencie surtout des autres, c'est l'animation 3D et la modélisation. D'ailleurs, la plupart des tutos que vous trouverez sur Blender portent sur ces sujets. Son puissant moteur de rendu en a sous le capot, et donne vie à toutes les animations. La version 3.0, déjà bien complète, est sortie en décembre dernier mais vous pourrez toujours contribuer à l'améliorer grâce à la possibilité de créer vos propres outils et add-ons, via Python.

Lien : blender.org

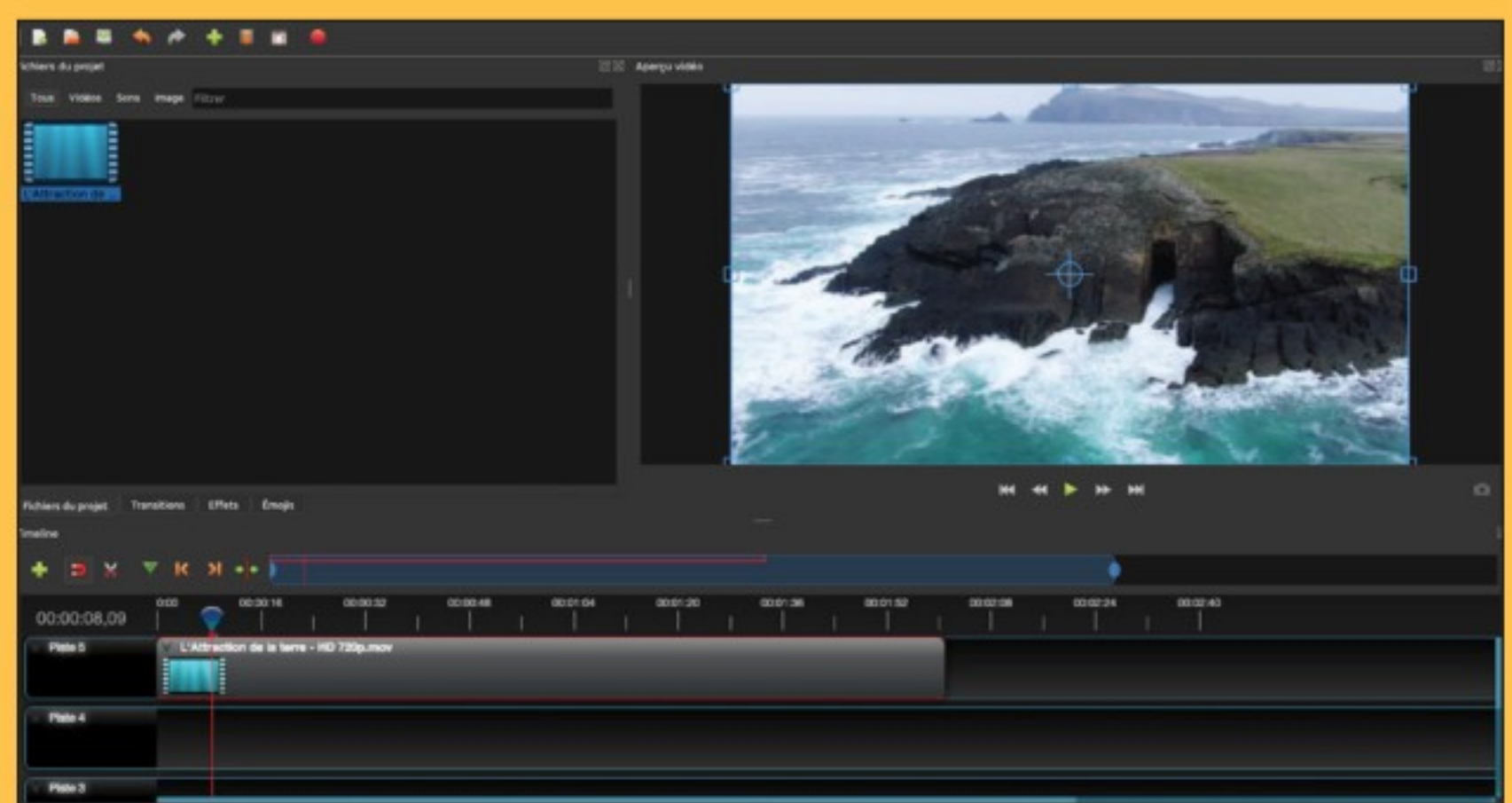


OPENSLOT > POUR LES DÉBUTANTS

La mission d'OpenShot : simplifier l'usage des fonctionnalités avancées. Pour vous y aider, ce logiciel propose des modèles intégrés, un aperçu en temps réel et tout le nécessaire pour vous aider à apprendre à monter vos vidéos. Vous pouvez même rogner vos vidéos pour les recadrer. Vous aurez également accès à de nombreux effets de titre et à un nombre de superpositions illimité. N'en abusez pourtant pas, sous peine de les rendre illisibles !

Son principal défaut : l'export est parfois un peu long. Mais comme il vous permet de produire des vidéos en 4 K UHD ou en 2,5 K QHD, entre autres, on ne devrait pas trop lui en vouloir. Didacticiel de départ, options superflues éliminées, bibliothèque d'effets vidéo et d'animations... Il a tout pour vous aider à vous faire la main sur vos premiers films (et les suivants). Petit bonus sur la pellicule : OpenShot est également disponible en français !

Lien : openshot.org/fr





POUR QUI ?

Bah, les amateurs de podcasts !

POUR QUOI FAIRE ?

Trouver rapidement ce qui vous intéresse grâce à des filtres efficaces.

TROUVEZ ET ÉCOUTEZ DES PODCASTS

Dénicher un podcast intéressant se révèle déjà parfois compliqué. En trouver qui traitent de sujets particuliers relève là de l'exploit. Sur ce terrain, le service Listen Notes va vous donner un sérieux coup de main.



Si vous êtes fan de podcast, vous utilisez probablement les services d'Apple, Google, Spotify ou encore de Deezer pour trouver votre bonheur. Las, à moins de savoir déjà assez précisément ce que vous recherchez comme le nom de la station de radio ou encore celui de l'émission ou de l'animateur, votre recherche peut vite tourner au cauchemar. Sauf à utiliser Listen Notes. Gratuit, ce service en ligne se présente comme un moteur de recherche bien plus poussé que ce que l'on trouve sur les autres plateformes. Vous pouvez bien sûr opérer une requête sur un nom ou le titre d'une émission, mais surtout, indiquer un thème comme « hacker », « ovni » ou encore « cold case » par exemple. Il suffira ensuite de jouer avec les filtres

proposés pour choisir une catégorie, une langue, un pays d'origine, etc. Pratique.

ÉCOUTE IMMÉDIATE OU DIFFÉRÉE

Listen Notes dispose de son propre lecteur audio pour écouter directement le podcast que vous avez déniché. Nul besoin donc de vous rendre sur une autre plateforme pour en profiter. Et, si vous vous inscrivez (gratuitement), vous pourrez alors l'enregistrer en l'ajoutant dans une liste de lecture pour l'écouter plus tard. Celle-ci contient un flux RSS. Vous pourrez ainsi la récupérer pour l'utiliser avec n'importe quel lecteur de podcasts, y compris sur un mobile puisque, à l'heure actuelle, Listen Notes n'est disponible qu'à travers un navigateur Web.

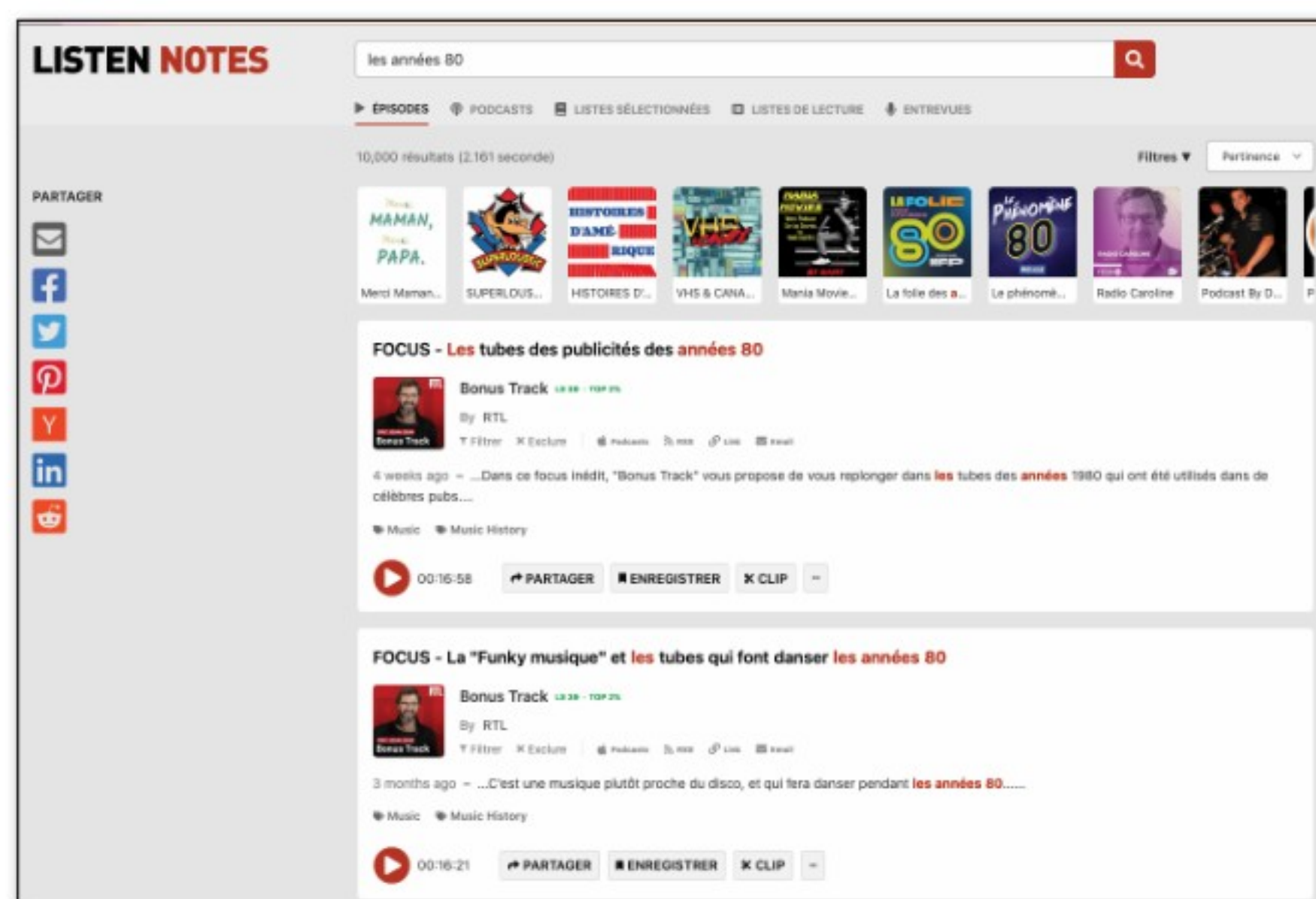
RECHERCHER DES PODCASTS À TRAVERS LE MONDE AVEC LISTEN NOTES

PRATIQUE



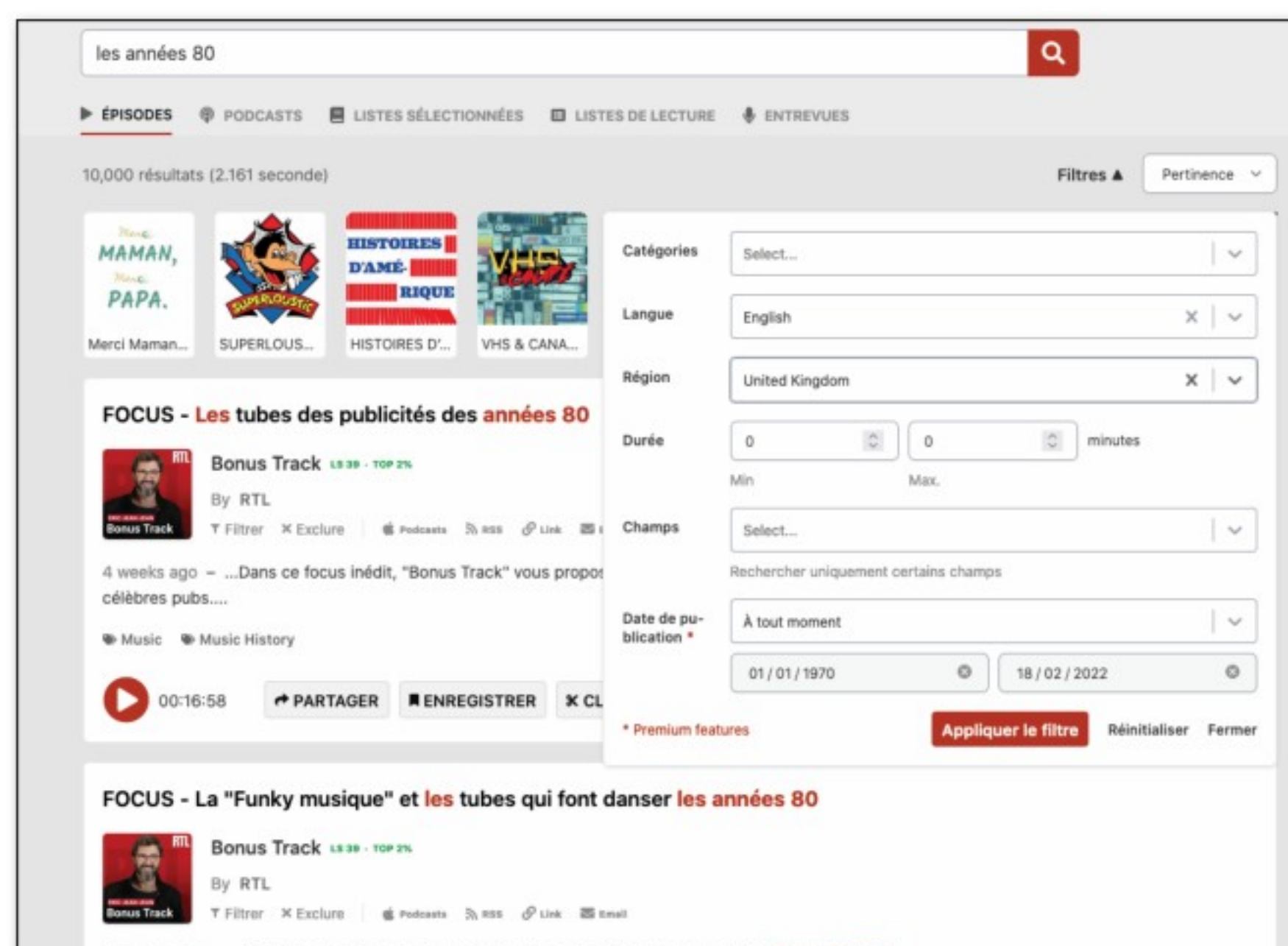
01 > TROUVER UN PODCAST

Une fois sur le site de Listen Notes, saisissez dans le champ de recherche l'objet de votre requête. Il peut s'agir d'un nom, d'un mot ou d'une phrase. Si les auteurs de podcast ont bien renseigné les tags dans le descriptif de leurs épisodes, les résultats proposés seront des plus cohérents. Une liste de podcasts s'affiche alors.



02 > UTILISER DES FILTRES

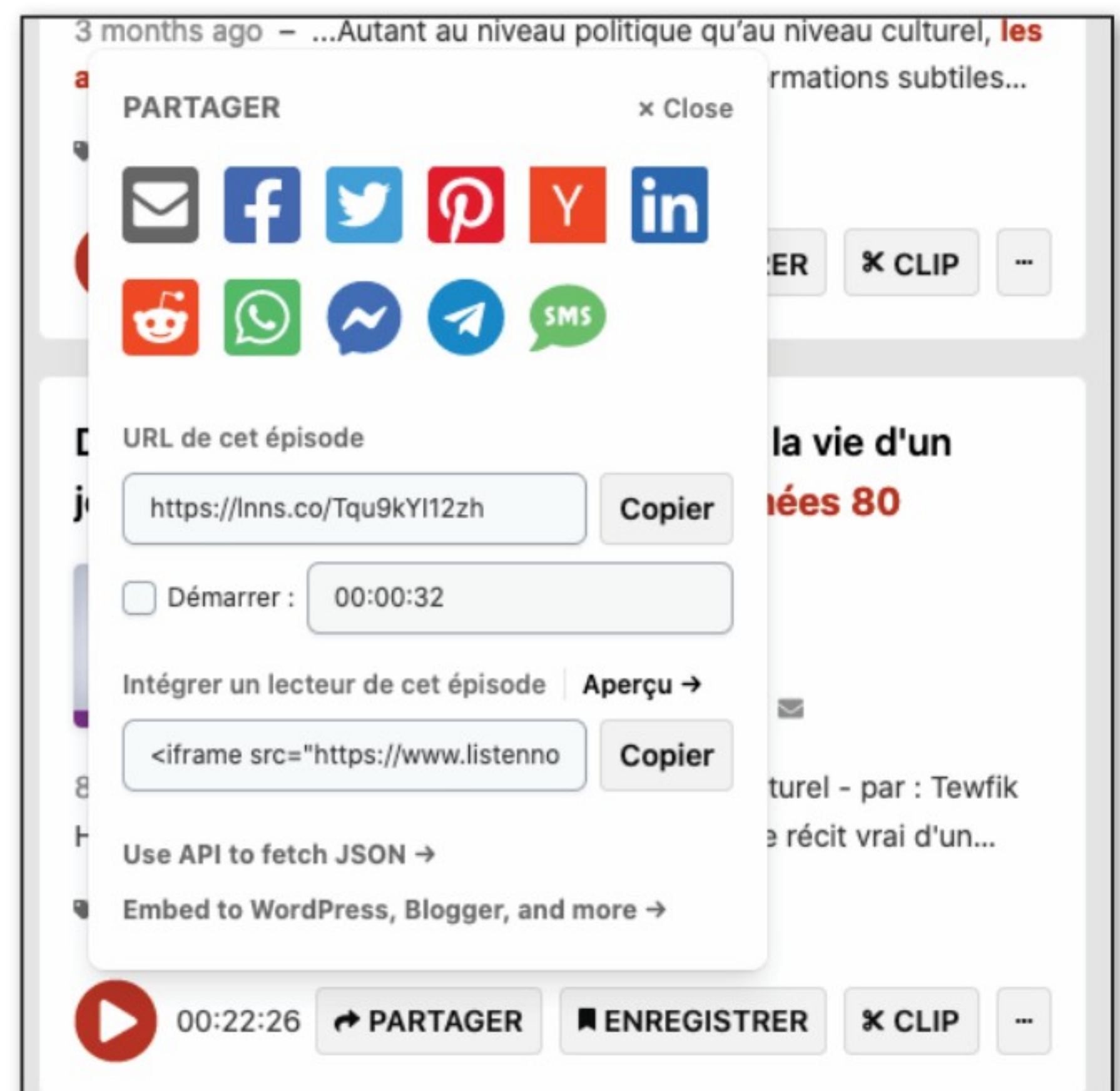
Pour affiner votre recherche, cliquez sur **Filtres** au sommet de la liste. Vous pouvez ici choisir une catégorie (football, jeux, science... attention, les catégories ne sont pas traduites en français), la langue du podcast, son pays d'origine ou même sa durée. Le filtre **Date de publication** est réservé à la version payante facturée environ 8 euros... par jour. Avec cette formule, Listen Notes vise avant tout les professionnels.



03 > PROFITER D'UN PODCAST

Vous avez trouvé votre bonheur ? Cliquez sur le bouton de lecture placé dans la fiche du podcast. Un mini lecteur s'affiche au bas de la

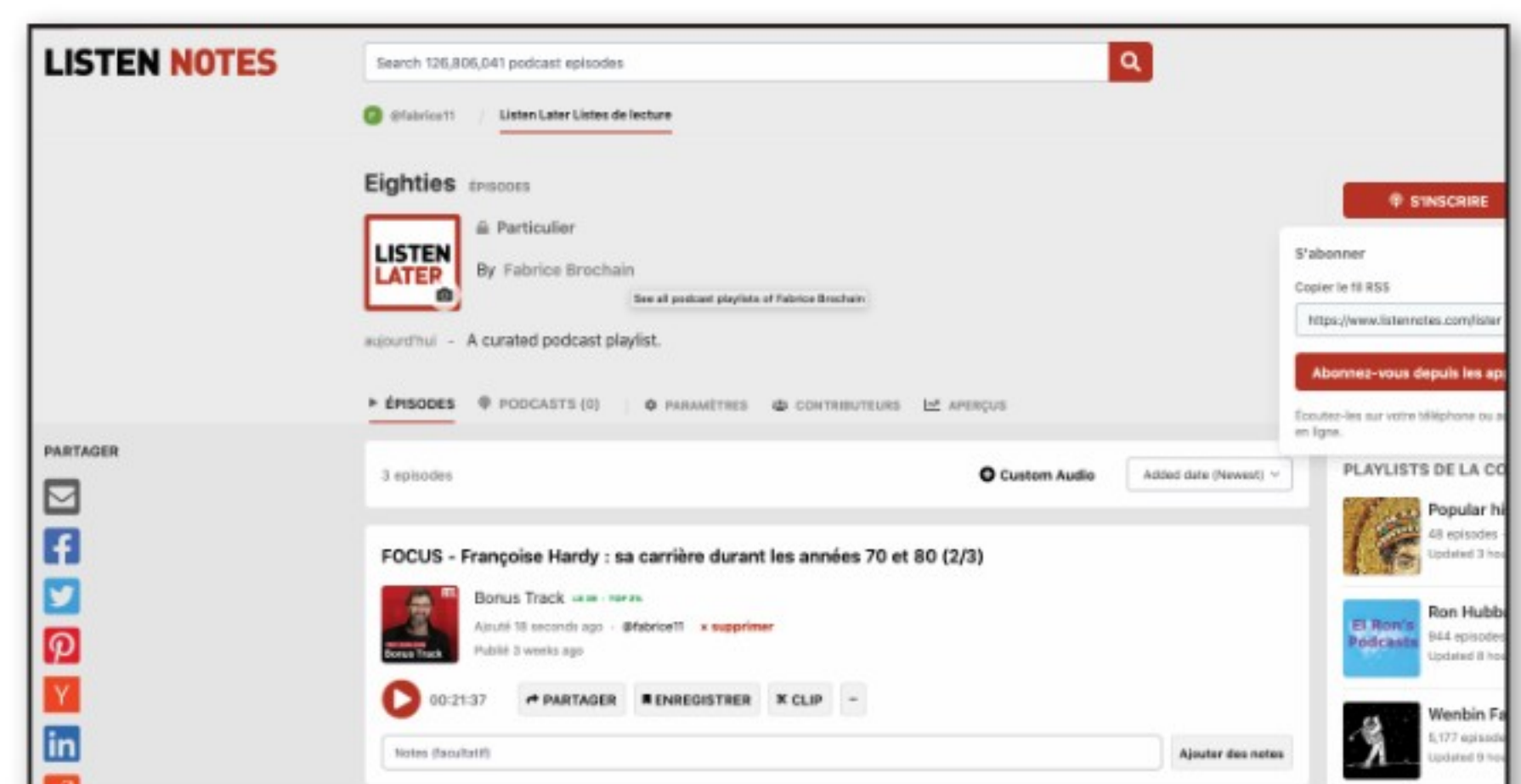
fenêtre. En cliquant sur le bouton **Partager**, vous accédez à toutes les options pour partager le podcast



sur les réseaux sociaux ou pour récupérer son URL ou encore pour profiter d'un lecteur prêt à l'emploi à intégrer sur votre site Web ou votre blog.

04 > CRÉER UNE LISTE DE LECTURE

Listen Notes permet de créer votre liste de lecture mise à jour automatiquement. Vous devez au préalable vous enregistrer en cliquant sur le bouton **Connexion** en haut à droite de la page.



Une fois connecté, cliquez sur le bouton **Enregistrer** du podcast souhaité puis sur **Créer une nouvelle liste de lecture**. Donnez-lui un nom et son accès (privé ou public). Cliquez de nouveau sur **Enregistrer** et cochez la case de votre liste de lecture. Vous pourrez retrouver vos podcasts dans la section **Listen Later** et copier le flux RSS qui s'y rattache.



CONTOURNÉZ LES LIMITATIONS DE PAYS

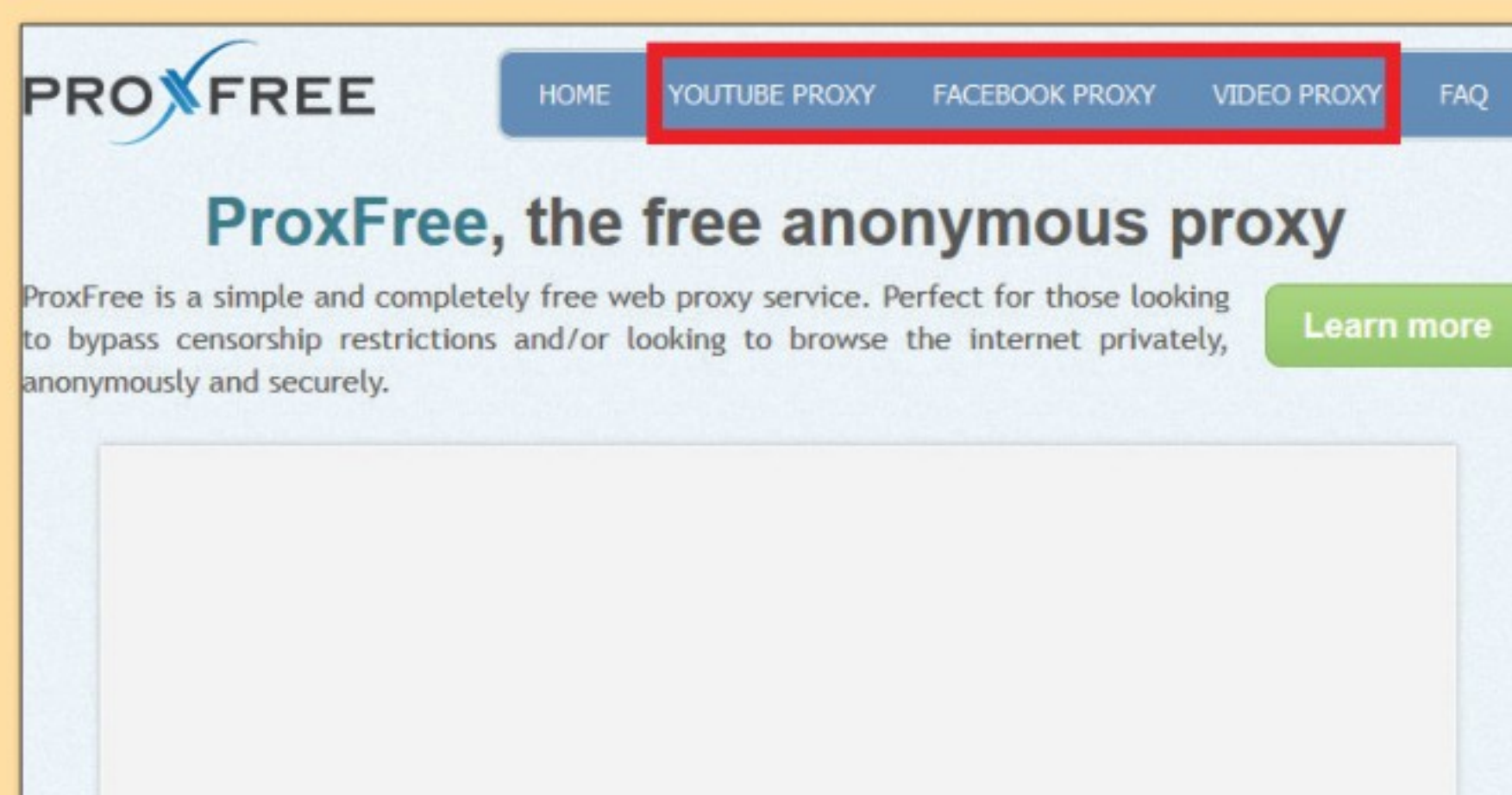


INFOS [ProxFree]
Où le trouver ?
[www.proxfree.com]
Difficulté :

Vous voulez accéder à une Vidéo YouTube indisponible en France ? Ou vous connecter à Facebook depuis un pays où le réseau social est inaccessible ? Passez par ProxFree.

01 > CHOISIR UN PROXY

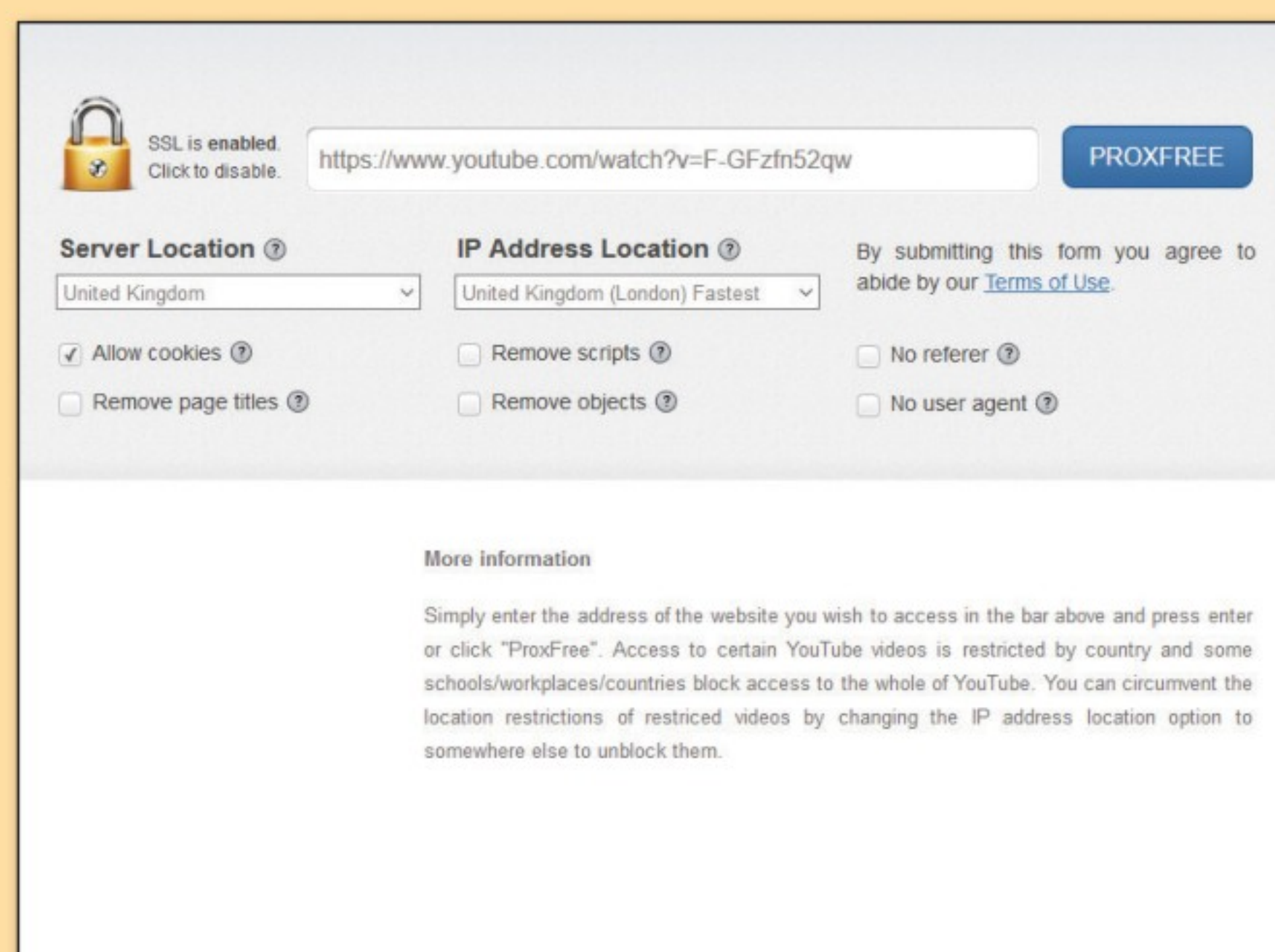
ProxFree dispose de trois types de proxy : **YouTube**, **Facebook** et **Video**. Même si les interfaces sont identiques, il est nécessaire de choisir le bon onglet pour procéder



au déblocage, sous peine d'échouer. **Video** englobe des plateformes comme Vimeo, Dailymotion, Vevo, Metacafe ou encore Vube.

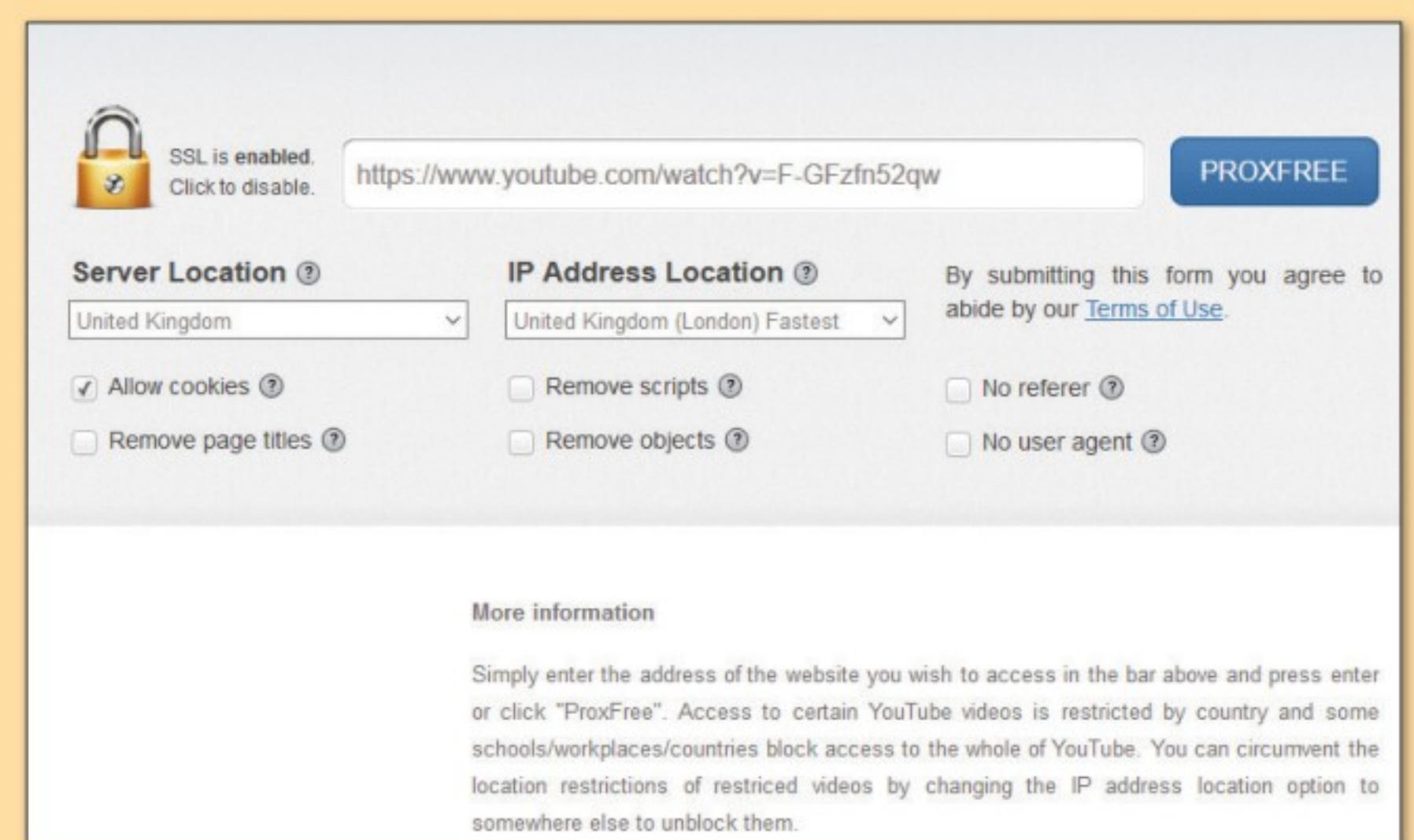
02 > DÉBLOQUER YOUTUBE

Cliquez sur **YouTube proxy** et collez le lien de la vidéo inaccessible. Changez ensuite **Server Location** pour un pays où la diffusion de la vidéo est autorisée. Dans notre exemple, nous choisissons **United Kingdom**, seul pays où cela fonctionne. L'**IP Address Location** est choisie automatiquement par le service. Validez avec **ProxFree** pour lancer le visionnage.



03 > DÉBLOQUER FACEBOOK

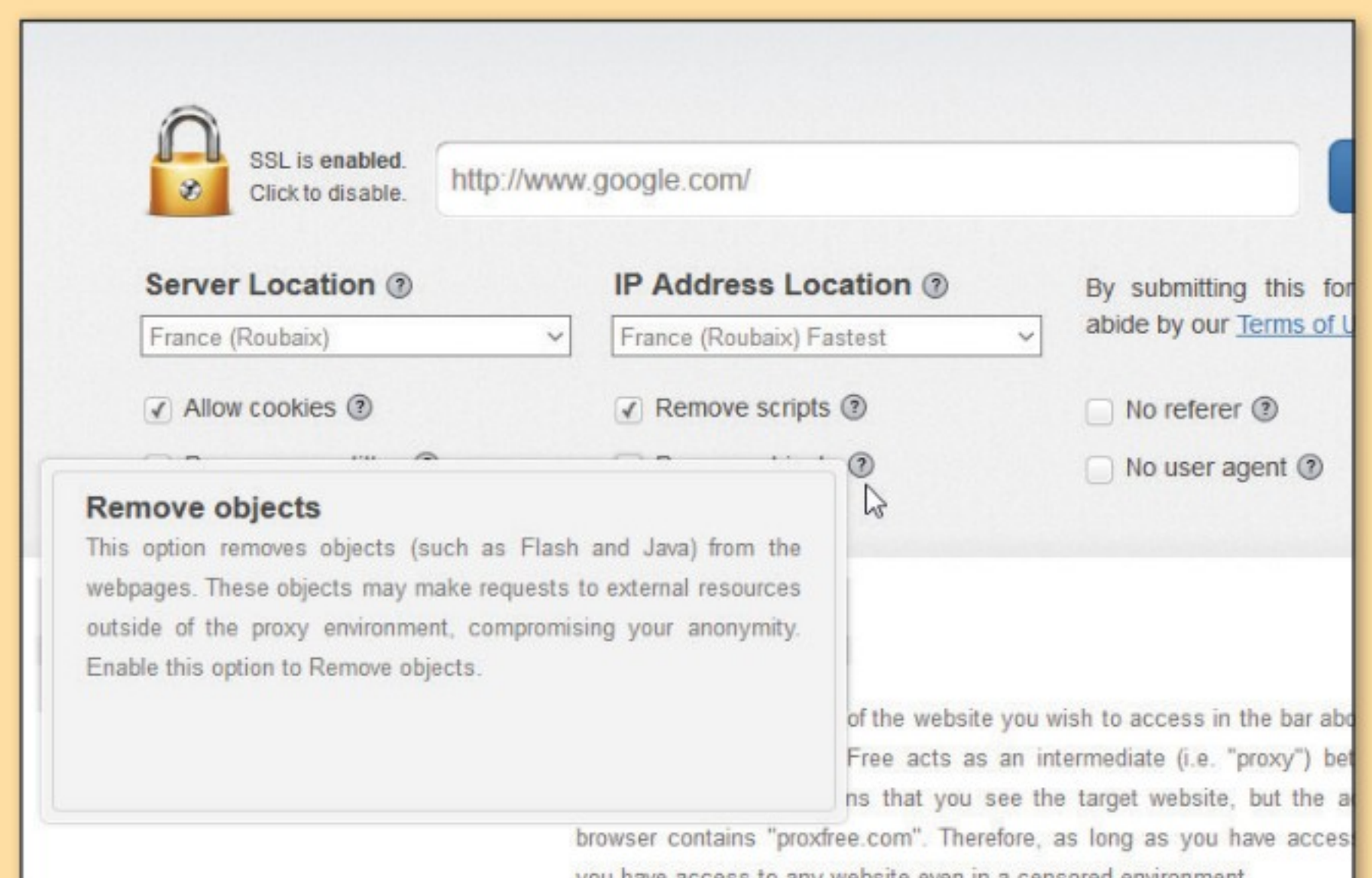
Dans certains pays, le célèbre réseau social n'est pas accessible. Cliquez sur l'onglet **Facebook proxy**. Il ne s'agit pas de débloquent une page en particulier, mais



bien le site entier. Vous n'avez donc rien à faire, si ce n'est choisir les options de sécurité (voir étape suivante), et cliquer sur **Proxfree**.

04 > PROTÉGER SA VIE PRIVÉE

Les six cases disponibles sont autant de protections supplémentaires de la vie privée. Cochez ou décochez-les à loisir, mais sachez que selon les cas, comme pour les scripts, cela peut empêcher le bon fonctionnement de la page. Référez-vous aux explications (en anglais), en posant le pointeur de souris sur le point d'interrogation, et faites des essais en cas de problème.



TÉLÉCHARGEZ DU CONTENU D'INSTAGRAM

PRATIQUE



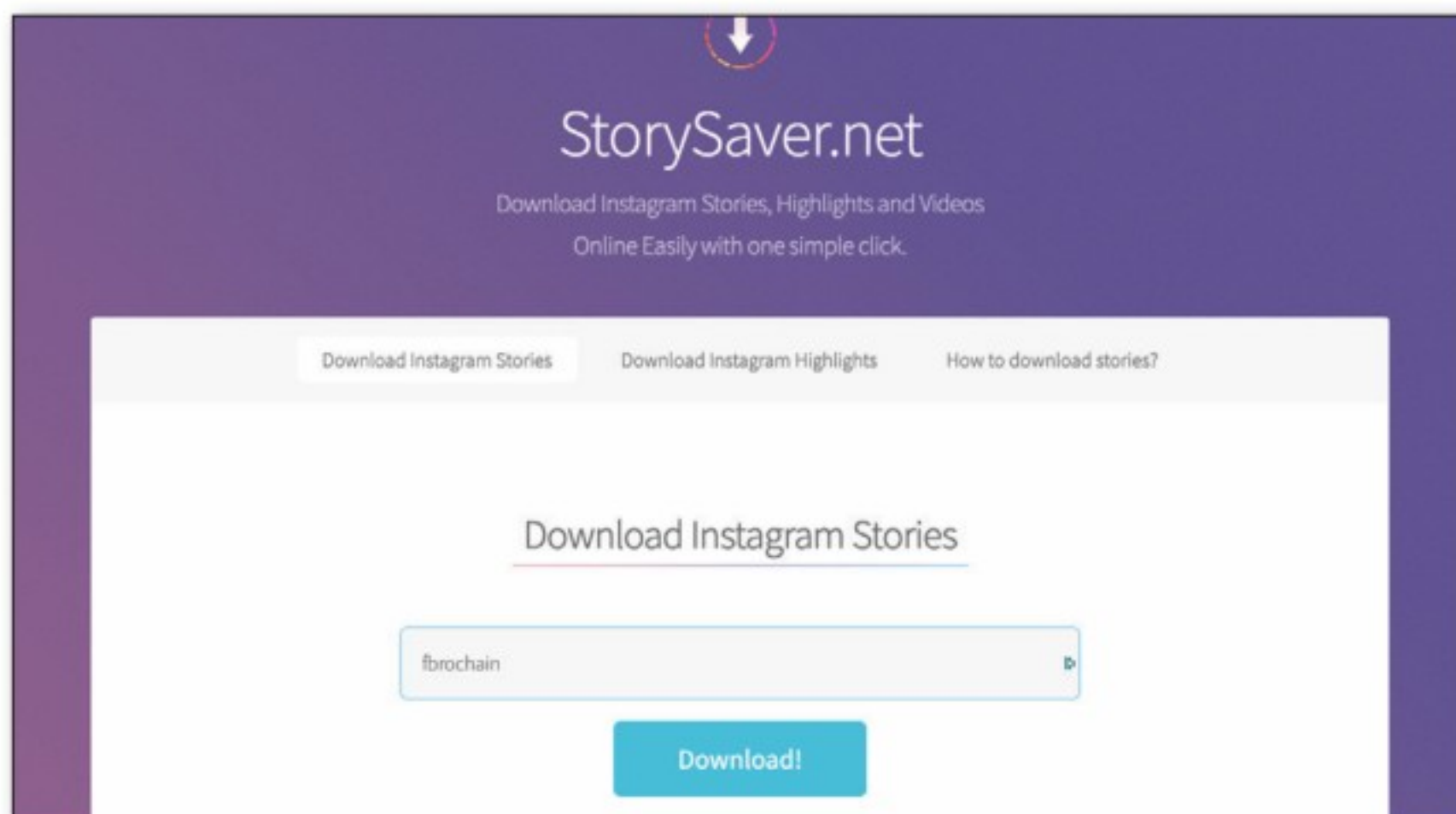
Vous voulez récupérer une story ou une vidéo publiée par un proche sur Instagram ? Un ordinateur, un navigateur Web et quelques clics suffisent.



INFOS [**StorySaver**]

Où le trouver ? [storysaver.net]

Difficulté : 🧑🏻 🧑🏻 🧑🏻

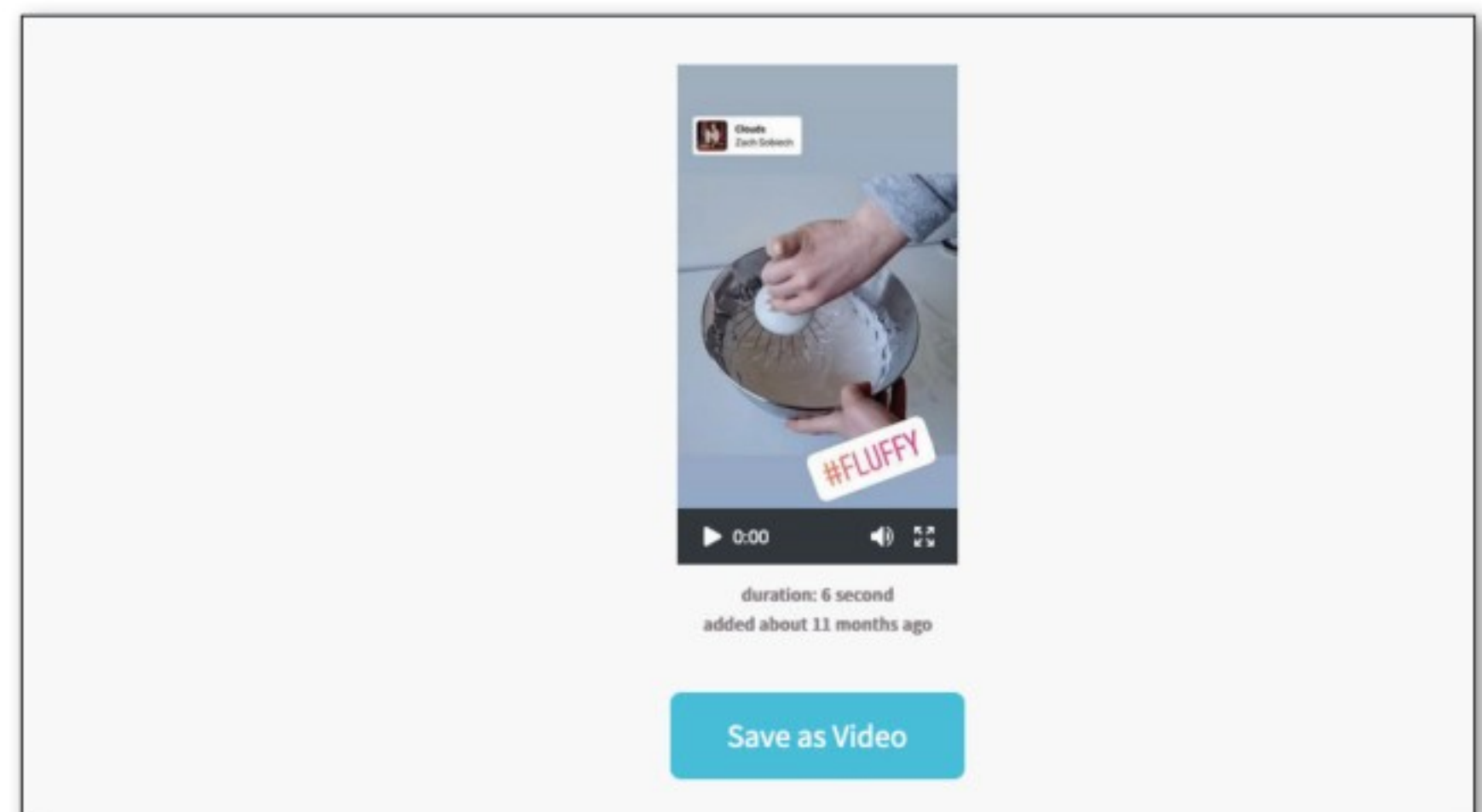


01 > REPÉRER LE COMPTE

StorySaver est un service Web qui va contourner l'interface d'Instagram pour se focaliser sur les contenus. Rendez-vous tout d'abord sur le site à partir de n'importe quel navigateur Web. Indiquez ensuite dans le champ au centre de la page le nom du compte où se situent les éléments à récupérer et cliquez sur **Download**.

02 > RAPATRIER PHOTOS ET VIDÉOS

Après quelques secondes, le compte est identifié. Faites défiler la page pour repérer dans la liste la story que vous souhaitez récupérer puis cliquez sur le bouton **Save as photo** ou **Save as video** selon le cas. Le fichier est instantanément téléchargé. Attention, l'opération n'est pas possible avec les comptes privés.



ÉLIMINEZ UN ÉLÉMENT GÊNANT D'UNE PHOTO

PRATIQUE



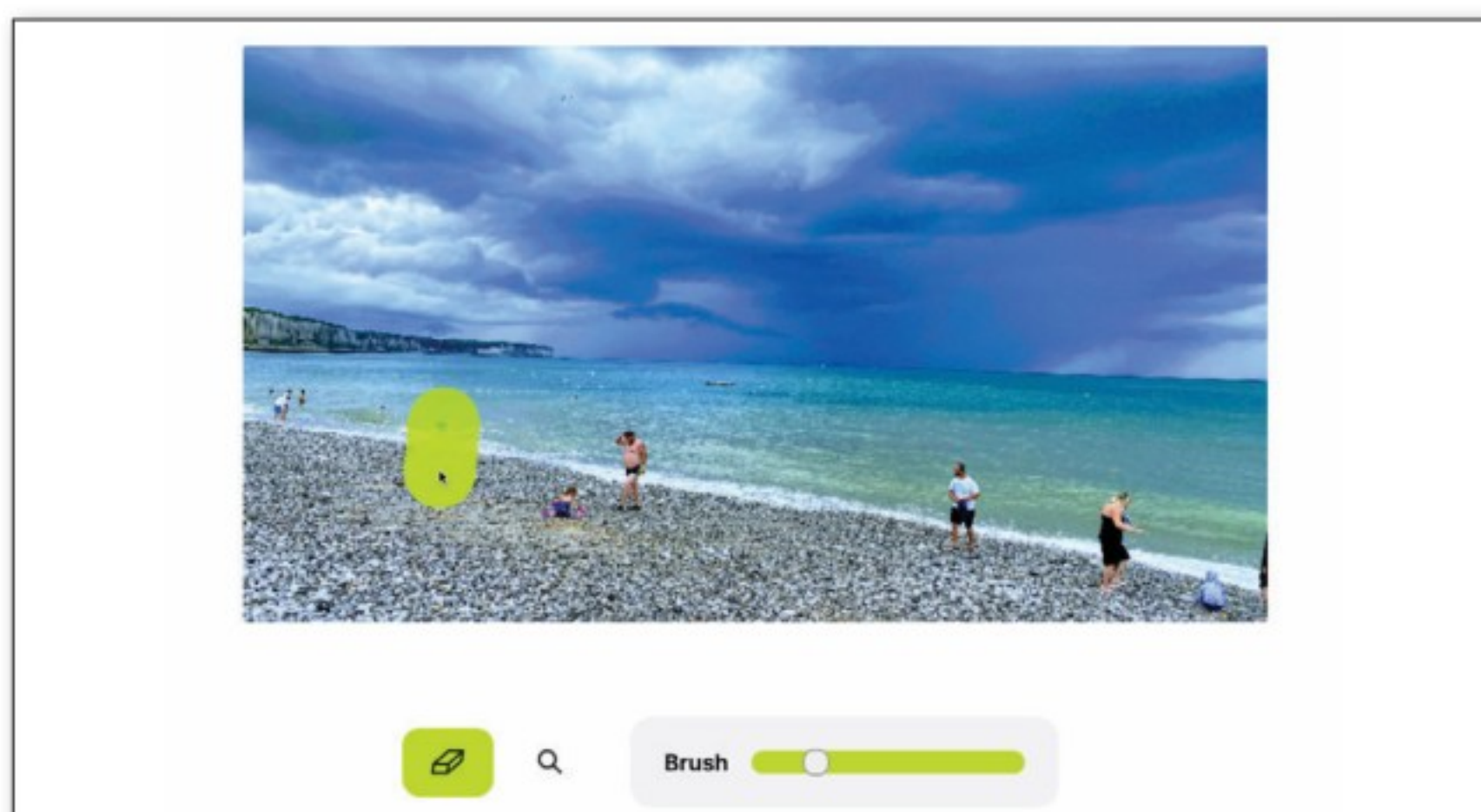
Google n'est pas le seul à disposer de la fameuse « gomme magique » pour supprimer proprement des éléments sur un cliché. Essayez le service gratuit Cleanup.pictures.



INFOS [**Cleanup.pictures**]

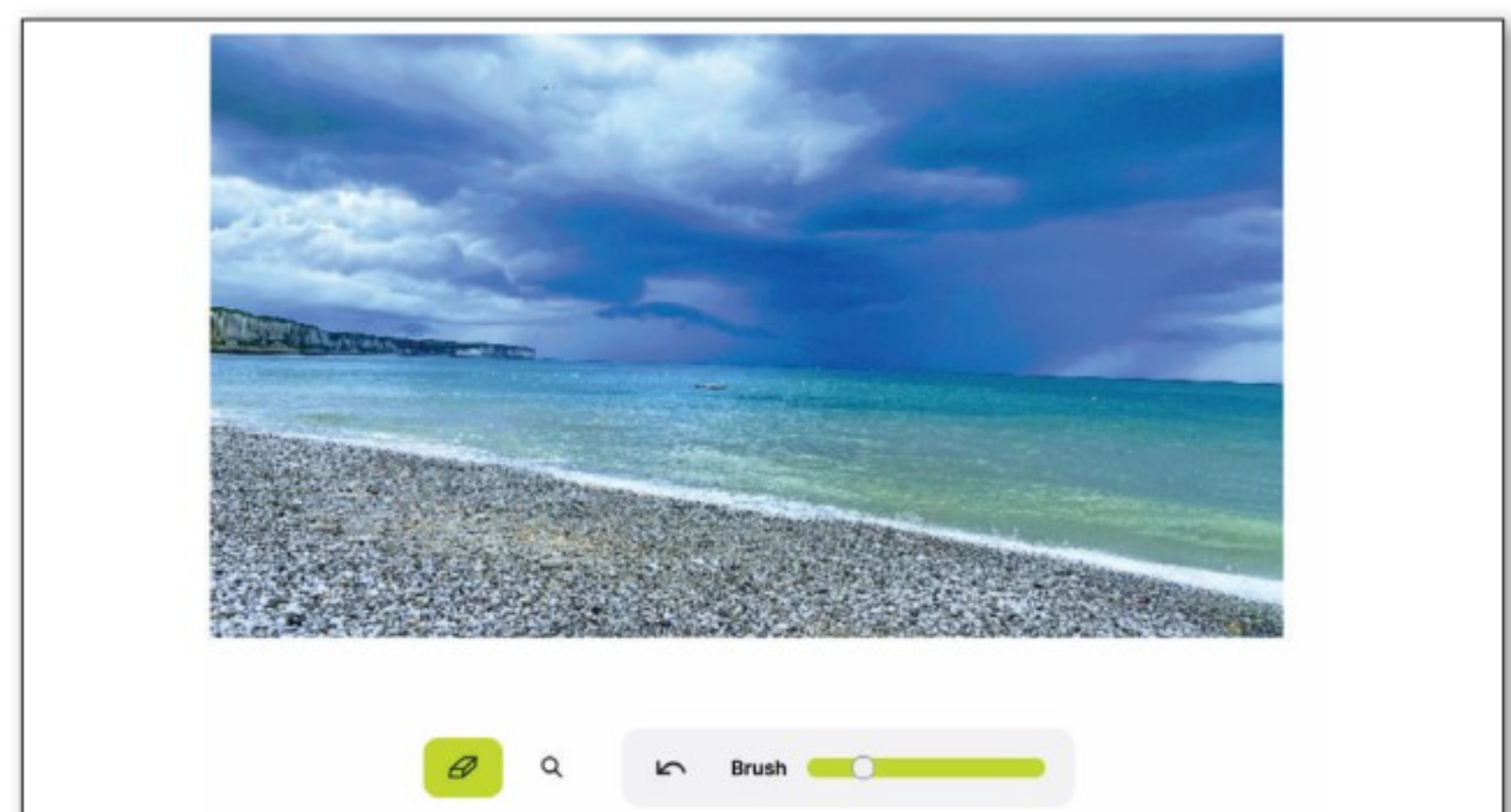
Où le trouver ? [<https://cleanup.pictures>]

Difficulté : 🧑🏻 🧑🏻 🧑🏻



01 > DÉSIGNER LES ÉLÉMENTS À SUPPRIMER

Rendez-vous sur le site de cleanup.picture. Faites ensuite glisser votre fichier image dans le cadre placé au centre de la page. Elle s'affiche tout de suite. Surlignez à présent les éléments à supprimer. Vous pouvez augmenter ou réduire la taille de la brosse à l'aide du curseur placé sous l'image.



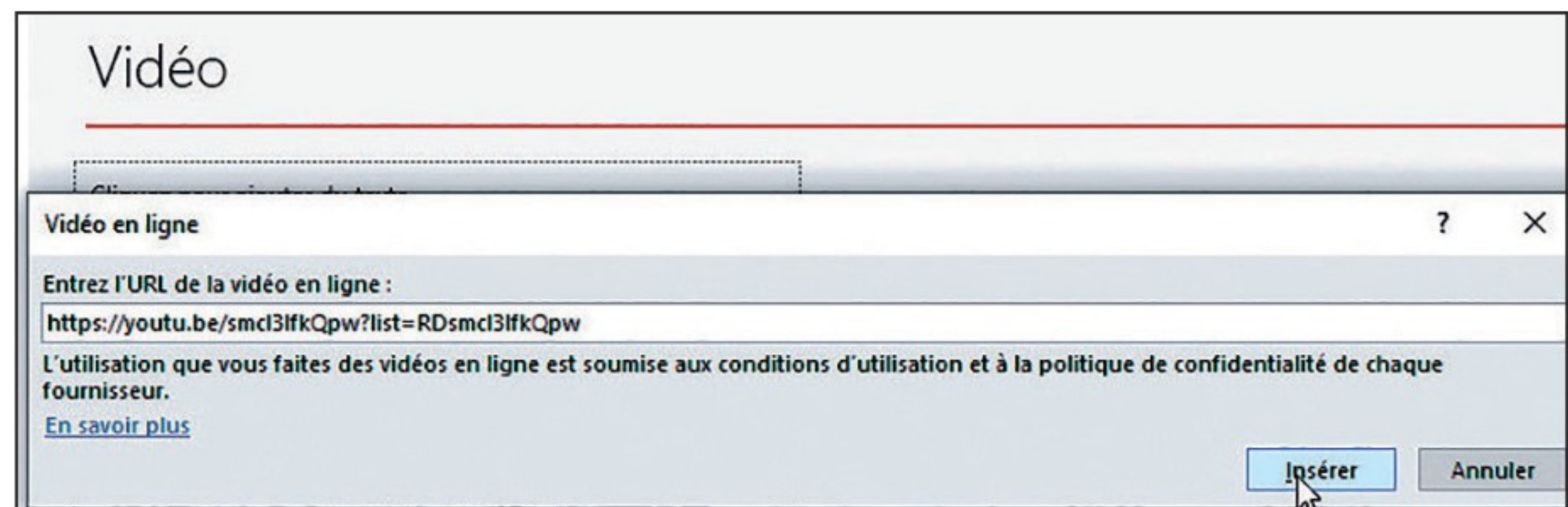
02 > RÉITÉRER L'OPÉRATION

Dès que vous relâchez le bouton de la souris, l'IA de Cleanup.picture se met en branle pour analyser l'image et en effacer les éléments sélectionnés. Vous pouvez recommencer l'opération pour supprimer d'autres parties. Si vous n'êtes pas satisfait, un clic sur la flèche pointant vers la gauche permet d'annuler la correction. Cliquez sur le bouton **Download** en haut de la page pour récupérer le fichier modifié.



Insérer une vidéo YouTube > AVEC POWERPOINT

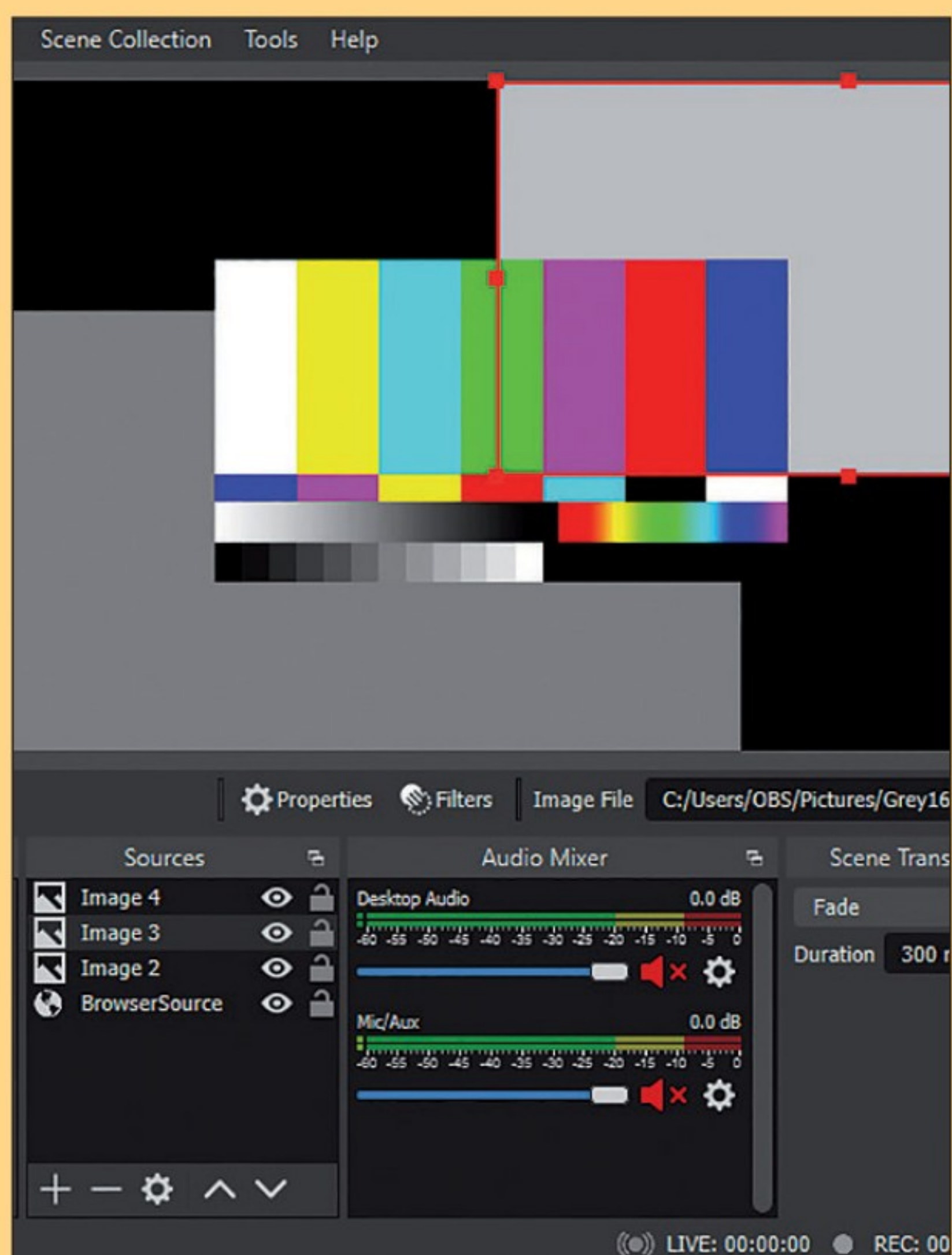
Il est possible d'insérer une vidéo YouTube dans votre présentation, pour la rendre plus vivante. Pour cela, ouvrez la vidéo sur YouTube, et copiez son URL (clic droit, **Copier l'URL de la vidéo**). Dans PowerPoint, placez-vous sur la diapositive voulue, et dans l'onglet Insertion cliquez sur **Vidéo > Vidéo en ligne**. Collez l'URL dans le champ affiché, et cliquez sur **Insérer**. Après un bref temps de chargement, votre vidéo apparaît sur votre diapositive.



Capture et stream de jeux vidéo > AVEC OBS STUDIO

Si l'envie de diffuser vos parties de jeux vidéo sur la toile vous titille, il vous faudra un bon logiciel d'enregistrement/ diffusion. La Rolls du payant s'appelle Xsplit (dans sa version premium), mais il existe un concurrent gratuit et Open Source tout aussi performant : OBS Studio. Hautement paramétrable et personnalisable, via un système de plugins, il saura satisfaire les utilisateurs les plus exigeants.

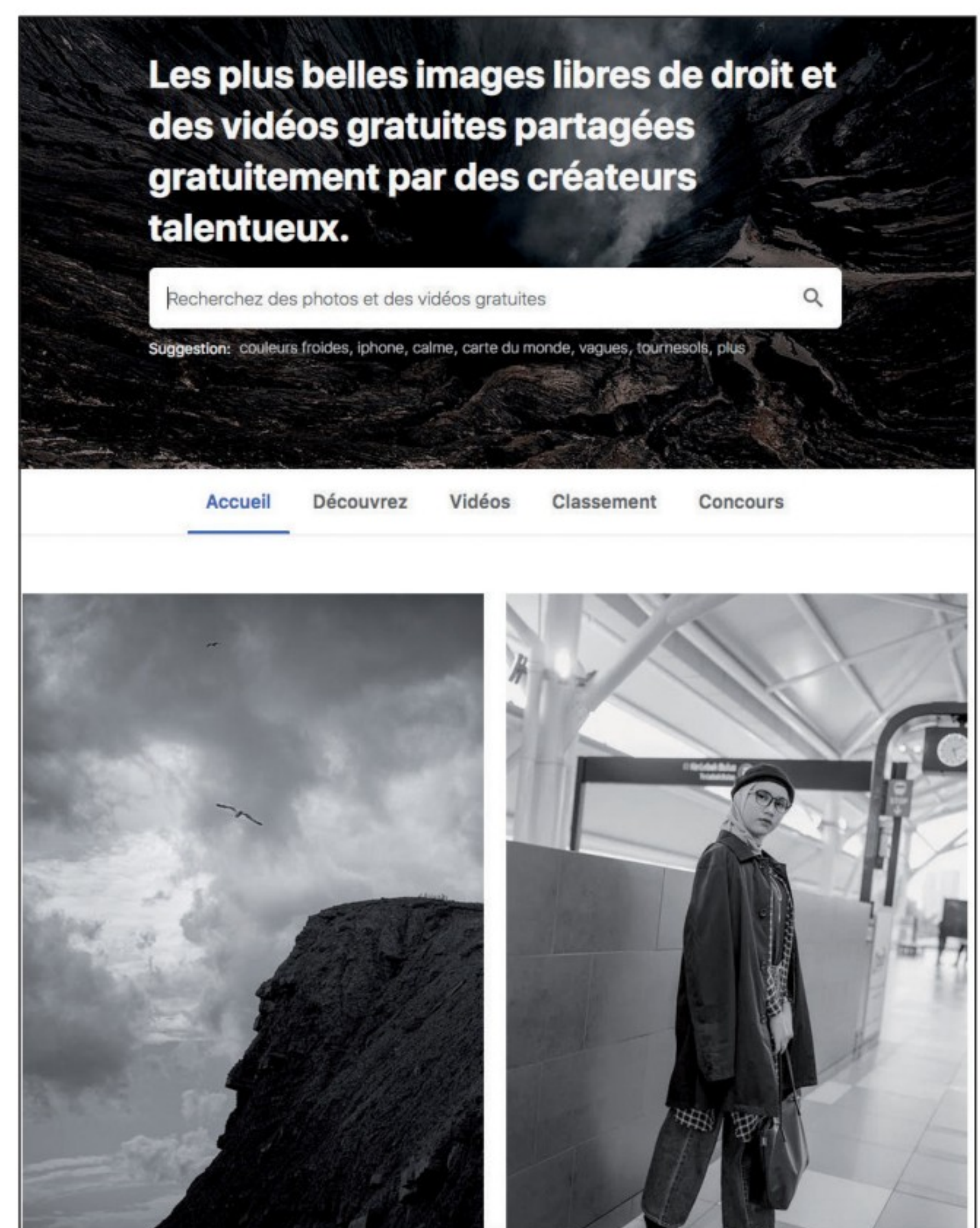
Lien : <https://obsproject.com>



Banque d'images libres de droit > AVEC PEXELS

Au moment d'illustrer votre article de blog, le problème est toujours le même : s'assurer que l'image choisie est bien libre de droits. Il existe certes des critères spécifiques dans la recherche de Google Images, mais le plus simple est encore d'utiliser un service proposant uniquement des photos de ce genre. Pexels en contient plus de 25 000, classées par catégories. Le système de recherche est pertinent, et il est même possible de chercher par couleur dominante.

Lien : www.pexels.com





Le nouveau site
des utilisateurs
ANDROID



Des dizaines de tutoriels et
dossiers pratiques



Mobiles &
Tablettes :
des tests complets !



Sélection des
meilleures applis
+ des vidéos
et du fun !



Android MT

S o l u t i o n s & A s t u c e s

www.android-mt.com



NOUVEAU
SITE !





ELIFE 2K+ : CAMÉRA DE SÉCURITÉ COMPLÈTE À MOINS DE 150 €

FLEXIBLE, FIABLE ET FACILE À UTILISER, CETTE CAMÉRA SUR BATTERIE EST NOTAMMENT DOTÉE D'UN ENSEMBLE DE FONCTIONNALITÉS PROFESSIONNELLES, UNE QUALITÉ VIDÉO ULTRA-CLAIRE, UNE VISION NOCTURNE COULEUR, UNE DÉFENSE ACTIVE, ...

Destinée aux particuliers, la nouvelle caméra de sécurité de la marque EZVIZ présente un ensemble de caractéristiques alléchantes pour un prix étonnamment contenu. À moins de 150 euros, elle propose notamment des fonctionnalités que l'on retrouve le plus souvent sur la gamme supérieure : batterie permettant une autonomie en veille allant jusqu'à 7 mois, vidéo 4MP, vision nocturne couleur, conversation bidirectionnelle et une défense active avec sirène et lumières stroboscopiques. Outre sa batterie de 10400 mAh, son module Wi-Fi est directement intégré, ce qui rend son installation sans câble ultra-simple, en intérieur comme en extérieur. Fonctionnant comme une unité autonome, cette caméra est aussi



Prix : 149 €
Lien : www.ezviz.com/fr

CARACTÉRISTIQUES

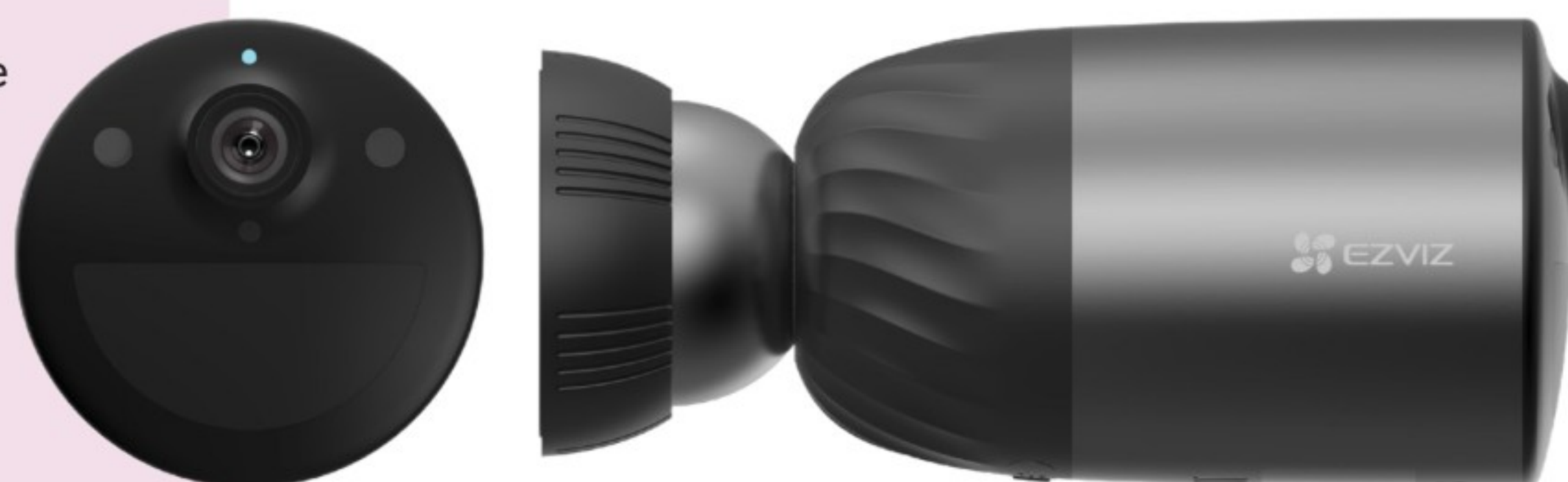
- **Destination** : Intérieur ou extérieur (norme IP66)
- **Communication** : Wi-Fi
- **Alimentation** : Batterie (10400 mAh)
- **Compatibilité** : Android, IOS
- **Capteur d'images** : Capteur CMOS 1/2,8» à balayage progressif de 4 mégapixels
- **Résolution maximale** : 2560 x 1440
- **Compression vidéo** : H.265/H.264
- **Nombre maximal d'images/sec** : 15
- **Portée maximale** : 10 mètres
- **Angle de vue** : 116°
- **Capacité de stockage** : carte 32 Go intégrée
- **Dimensions** : 10,5 x 6,3 x 6,3 cm
- **Poids** : 365 g
- **Couleur** : Gris
- **Autres** : Détecteur de mouvement et de personnes par IA, Microphone, Haut-parleur, Personnalisation de message d'alerte

AUTONOME, LA CAMÉRA SE FIXE SANS FIL, POSSÈDE SON MODULE WI-FI INTÉGRÉ, UNE BATTERIE ROBUSTE ET EST COMPATIBLE AVEC UN USAGE EXTÉRIEUR.

compatible avec les panneaux solaires de EZVIZ pour une recharge en continu.

SURVEILLANCE, DÉTECTION ET ALARMES

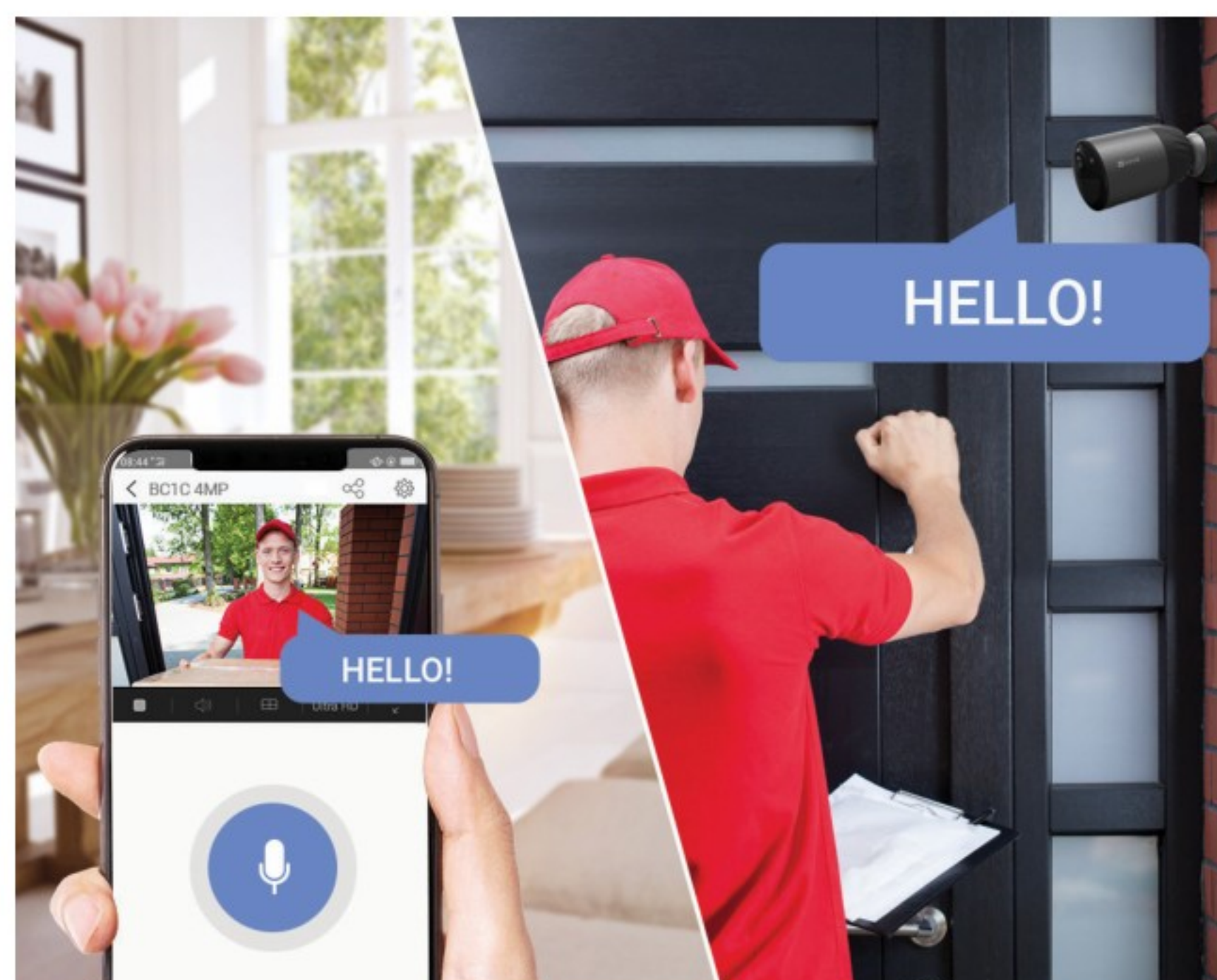
La vision nocturne est possible grâce aux projecteurs intégrés. Avec le capteur PIR et l'algorithme de détection, la caméra eLife 2K+ distingue les humains des autres objets en mouvement. Lors de la détection, les utilisateurs



recevront des alertes mobiles instantanées où qu'ils se trouvent et la caméra déclenchera une sirène puissante et des flashes stroboscopiques pour une dissuasion sur site. Les utilisateurs peuvent définir des plages horaires spécifiques pour la détection. Dès que la caméra EZVIZ eLife détecte la silhouette d'une personne, elle déclenche automatiquement une sirène et fait clignoter deux projecteurs pour lui faire savoir qu'elle a été détectée. Vous pouvez également créer des messages vocaux uniques pour l'accueil ou la dissuasion ainsi que communiquer en direct à distance. Le micro intégré permet bien sûr d'entendre ce qui se passe et se dit sur site.

À SAVOIR

eLife 2K+ est livrée avec une capacité de stockage eMMC de 32 Go. Le stockage en cloud EVZIZ est également disponible sur abonnement pour offrir si besoin une tranquillité d'esprit supplémentaire.



VIA L'APPLICATION, VOUS POUVEZ VOIR ET COMMUNIQUER AVEC LA PERSONNE DÉTECTÉE PAR LA CAMÉRA

DIS PAPA, C'EST QUOI CE DISQUE DUR CHIFFRÉ ?

FLEXIBLE, FIABLE ET FACILE À UTILISER, CETTE CAMÉRA SUR BATTERIE EST NOTAMMENT DOTÉE D'UN ENSEMBLE DE FONCTIONNALITÉS PROFESSIONNELLES, UNE QUALITÉ VIDÉO ULTRA-CLAIRE, UNE VISION NOCTURNE COULEUR, UNE DÉFENSE ACTIVE, ...

DataLocker sort son nouveau disque dur chiffré, le DL4 FE. Pas de solution logicielle tierce, de smartphone ou autre hardware connecté en double authentification pour déverrouiller la bête : un clavier digital vous permettra d'avoir accès à ses précieuses données. Plus simple donc, plus grand public, mais est-ce autant sécurisé ? Le DataLocker DL4 FE est disponible en deux options, SSD et HDD, avec des capacités de 500 Go, 1 To et 2 To pour les versions HDD et de 1 To, 2 To, 4 To, 7,6 To et 15,3 To pour les SSD.

Nous n'énumérerons pas tous les prix, mais pour avoir une idée, le modèle entrée de gamme à 1 To est au prix de 390 € et le SSD de 1 To à 620 €. Et pour les plus riches - ou pour ceux qui possèdent la collection complète des fichiers 8K de Poutine batifolant (plusieurs milliers d'épisodes!) -, l'option SSD de 15,3 To coûte quand même 4950 € !

JAMES BOND APPROUVE

L'interface peut être configurée en français, pour un ou plusieurs utilisateurs, et avoir des règles de complexité de mot de passe définies. L'obtention de la certification FIPS 140-2 rend l'appareil presque inviolable si ces règles sont bien utilisées, même par des moyens militaires de haut niveau. Une fonction à la James Bond, baptisée SilentKill, est proposée par DataLocker : un mot de passe spécial que vous donnez à ceux qui vous torturent rendra le lecteur inaccessible à jamais ! Le bémol : l'écran et les touches digitales sont vraiment petits. Pensez à utiliser un stylet plutôt que vos doigts.

Prix : à partir de 390 € Lien : datalocker.com





TOP 15

Logiciels
& services
GRATUITS

» TOP5 CLIENTS TORRENT

BITTORRENT > LE PLUS ANCIEN



BitTorrent est l'un des clients les plus connus. Il se vante de plus de 100 millions d'utilisateurs chaque mois. Mixte, il s'utilise en ligne, sur PC et également sur Android. Gérable

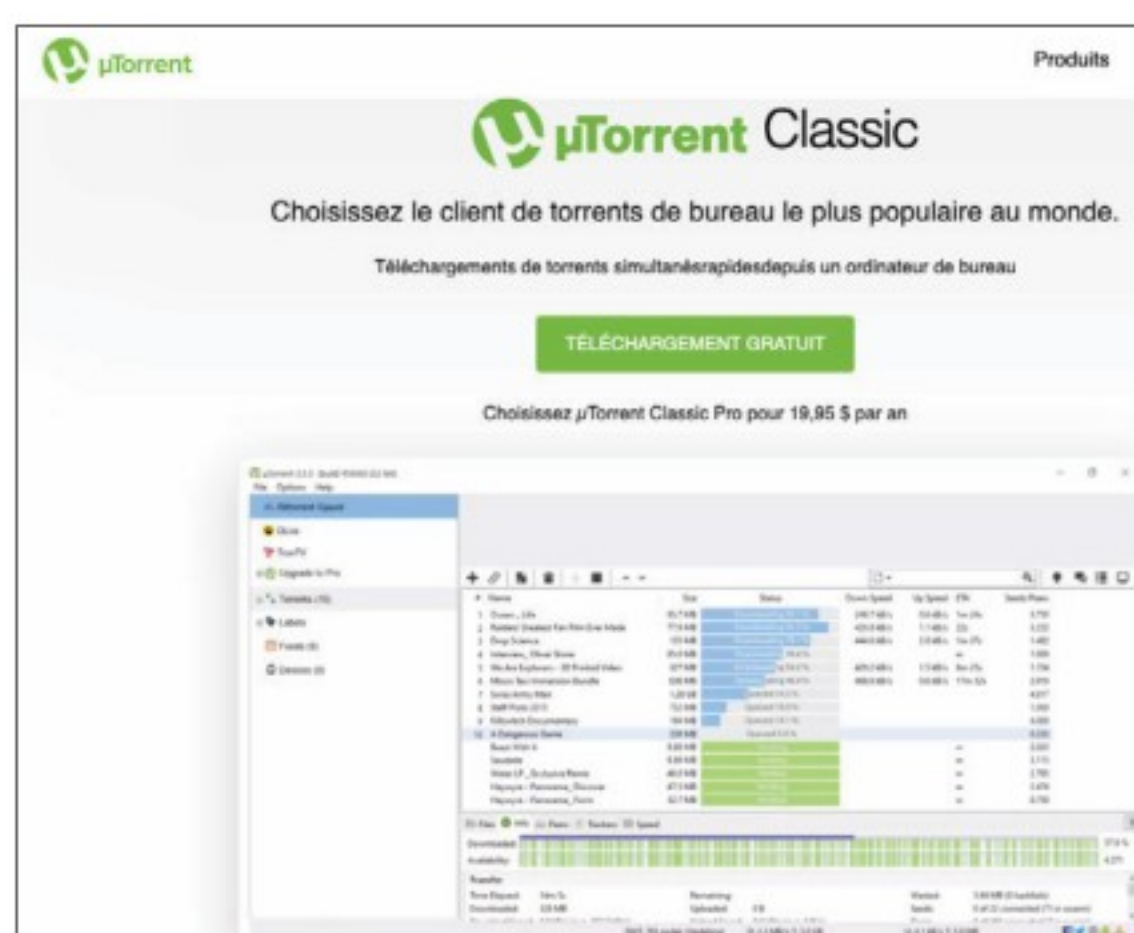
à distance, programmable, il comporte aussi des options pour économiser le réseau. Tout pour vous faciliter la vie !

Lien : bittorrent.com/fr

µTORRENT > LÉGER ET ADAPTABLE

Si vous cherchez un client léger, µTorrent a toute sa place chez vous. Les néophytes préféreront la version web, qui s'intègre dans le navigateur et permet un visionnage direct. La version Windows comporte plus de fonctionnalités (ajouter des torrents à distance, les programmer ou optimiser la bande passante). Il existe également en version mobile.

Lien : utorrent.com/intl/fr



QBITTORRENT

> L'OPEN SOURCE

qBittorrent est open source et cela lui confère un avantage en terme de transparence et de sécurité. Il est équipé d'un moteur de recherche et d'un lecteur multimédia intégré. Régulièrement mis à jour, il reste léger et simple à utiliser. Son interface ressemble d'ailleurs beaucoup à celle de µTorrent, avec des fonctions similaires.

Lien : qbittorrent.org



DELUGE > À PERSONNALISER



Deluge est un client très très léger... dans sa version de base. Si celle-ci est déjà complète, elle se distingue pourtant par l'ajout possible de nombreux plug-ins très appréciés des gros téléchargeurs. Il est

surtout conçu pour Linux (comme le prouve l'avancée des versions), mais il fonctionne aussi très bien sous Windows.

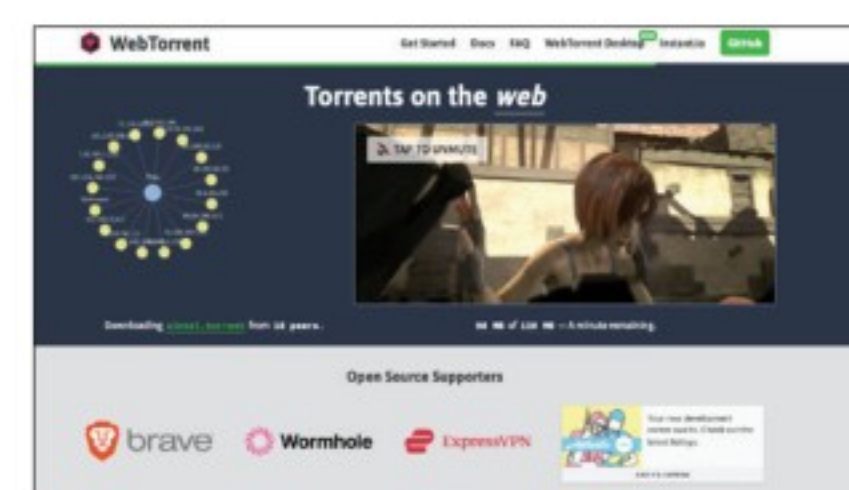
Lien : deluge-torrent.org

WEBTORRENT > LE PLUS ESTHÉTIQUE

À l'origine, WebTorrent était conçu uniquement pour les navigateurs et rédigé en JavaScript. Il a cependant été développé aussi pour les ordinateurs. Rapide, agréable à l'œil, il permet de visionner les vidéos en streaming.

Très léger, il ne consomme qu'une petite fraction de la puissance de calcul de votre ordinateur !

Lien : webtorrent.io

» TOP5 OUTILS
DE MONITORING

WATCH 4 FOLDER

> LE PLUS DIRECT

Il vous suffit de quelques étapes pour configurer le processus de surveillance de Watch 4 Folder. Ce qui ne limite pas pour autant ses capacités : il peut superviser une quinzaine d'événements différents, et effectuer diverses actions programmées. Par contre, en version gratuite, il ne pourra s'attarder que sur un dossier !

Lien : bit.ly/3pL1X62

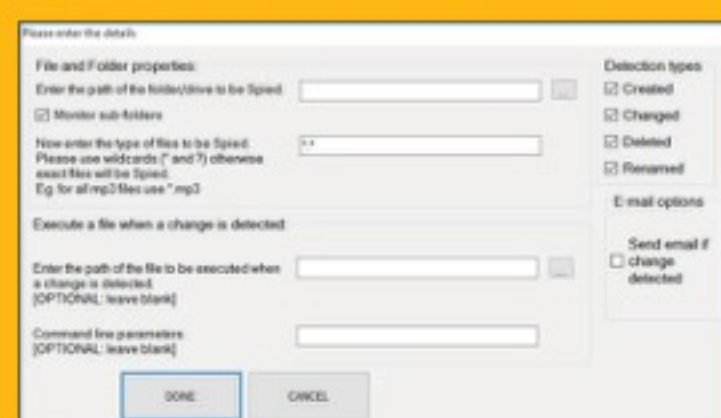


THEFOLDERSPY

> EN MODE ESPION

Cet outil de monitoring peut se transporter sur une clé USB et s'installer en mode incognito sur un appareil. Très léger, il surveille toutes les modifications de fichiers et dossiers et est entièrement automatisé. Une fois en place, vous n'avez plus qu'à regarder les journaux pour savoir ce qu'il s'est passé en votre absence.

Lien : bit.ly/3KhMQZI



FOLDERMONITOR

> SIMPLISSIME

Cet utilitaire très simple tient dans une seule fenêtre. Vous pouvez surveiller des disques locaux ou partagés, sélectionner le niveau d'alerte, les événements à noter... S'il n'a pas de kit d'installation, il ne comporte pas non plus d'options supplémentaires, qui pourraient compliquer son utilisation.

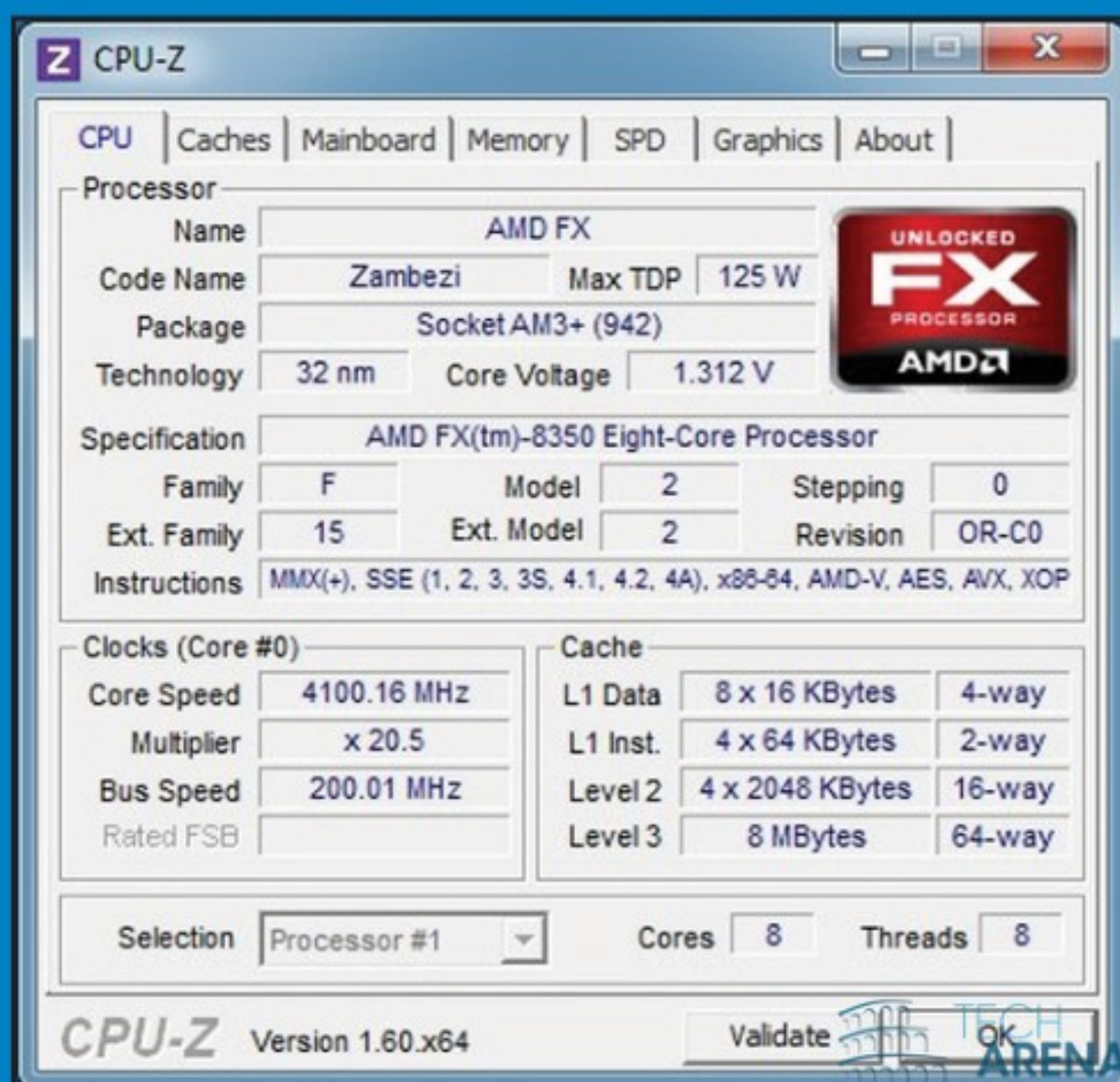
Lien : nodesoft.com/foldermonitor



CPU-Z

CPU-Z permet de connaître en temps réel la fréquence du CPU et du bus, la tension d'alimentation, la fréquence, les timings et les possibilités de la mémoire (via le SPD), etc. Disponible gratuitement sous Windows, il existe même une version pour les SoC des appareils Android.

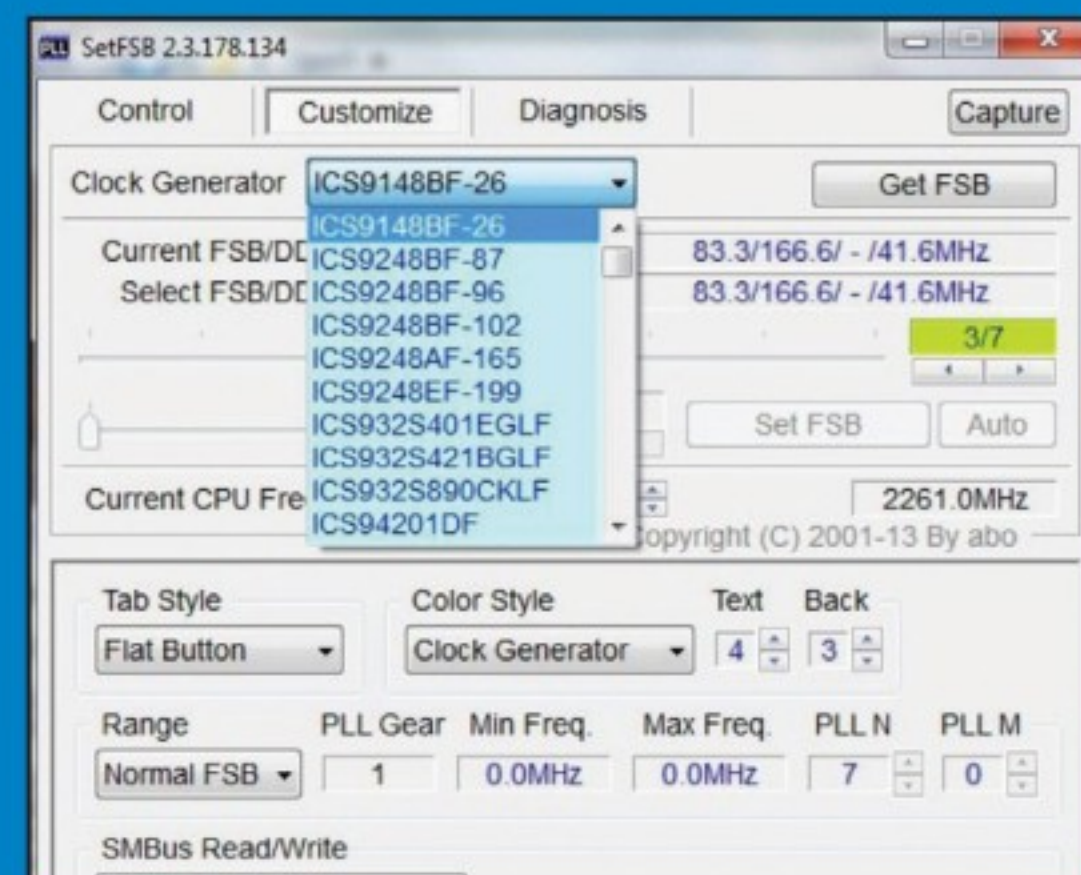
Lien : www.cpuuid.com



SETFSB

SetFSB permet de régler la fréquence du bus directement depuis Windows. Il est compatible avec énormément de cartes mères et nécessite simplement de connaître le PPL embarqué sur votre carte mère (Qwant est votre ami!).

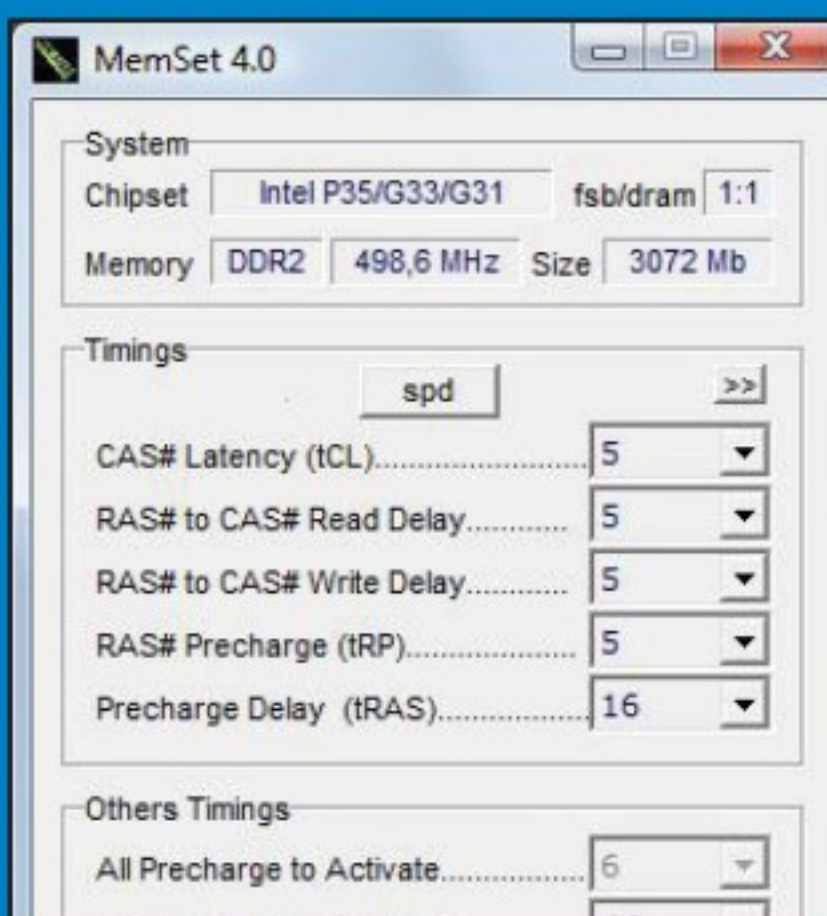
Lien : <https://frama.link/NotL3xCe>



MEMSET

Memset permet de régler finement les timings de la mémoire sans passer par les réglages du BIOS. Intéressant, car il fonctionne avec toutes les versions de Windows et évite de devoir redémarrer à chaque fois. Attention, à utiliser prudemment !

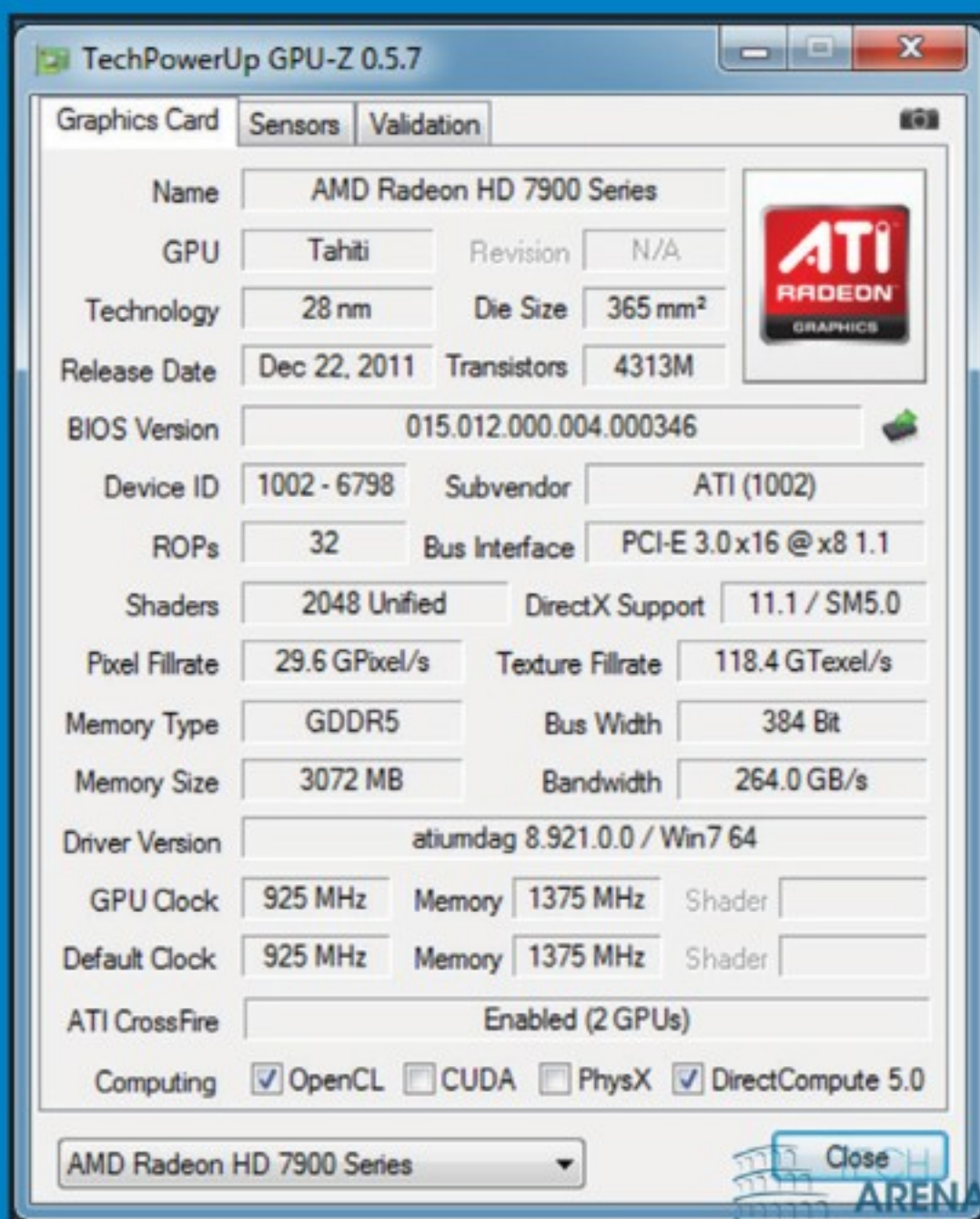
Lien : www.tweakers.fr/memset.html



GPU-Z

GPU-Z est dédié aux cartes graphiques et permet d'afficher des informations aussi variées que le nom exact de la carte et le type de GPU utilisé, la fréquence de la mémoire et des shaders, mais aussi le nombre de ROP, la largeur du bus mémoire, etc.

Lien : www.techpowerup.com/gpuz



RIVATUNER

RivaTuner fonctionne aussi bien sur les cartes graphiques NVIDIA que celle d'AMD. Il permet d'overclocker sans réelle limite de fréquence et de modifier indépendamment la fréquence des shaders et celle du GPU.

Lien : [www.guru3d.com/
content-page/rivatuner.html](http://www.guru3d.com/content-page/rivatuner.html)

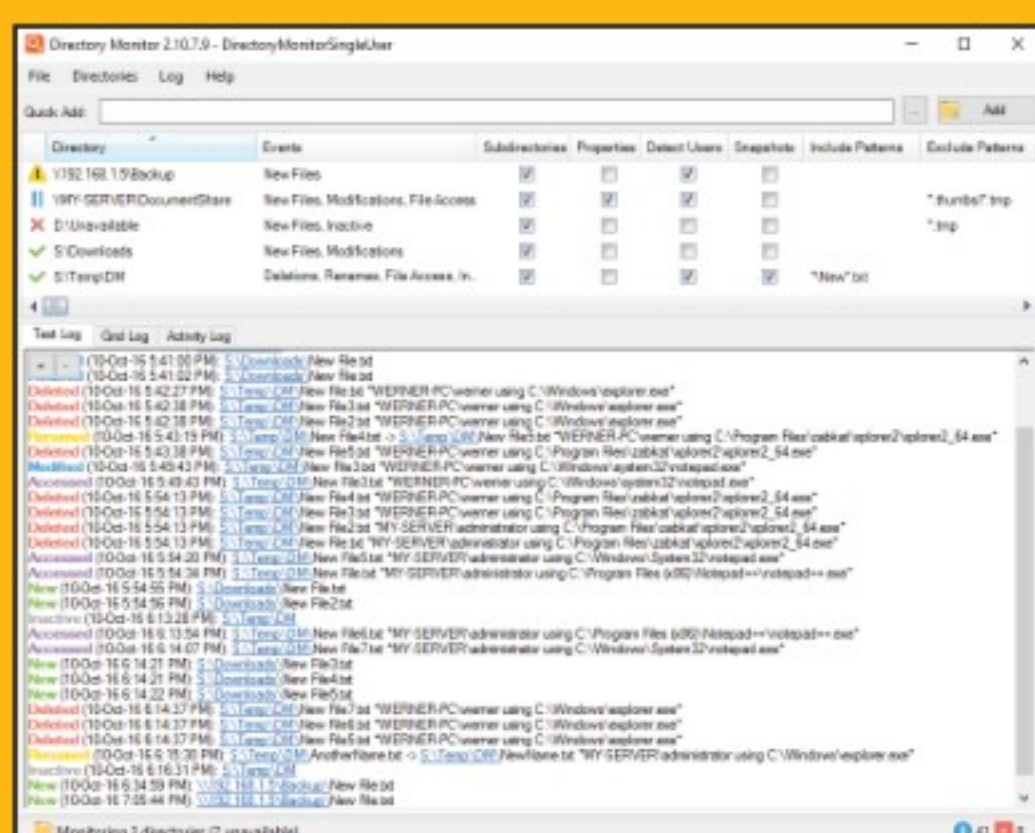


DIRECTORYMONITOR

> LE COMMUNICANT

DirectoryMonitor aime vous prévenir que quelque chose se passe sur votre ordinateur. Soit via un son (si vous ne voulez pas supprimer des fichiers par erreur), soit en vous envoyant des mails quand des modifications sont apportées. Léger, il peut passer inaperçu si vous le décidez. Vous pouvez aussi l'utiliser en mode réseau ou local.

Lien : directorymonitor.com

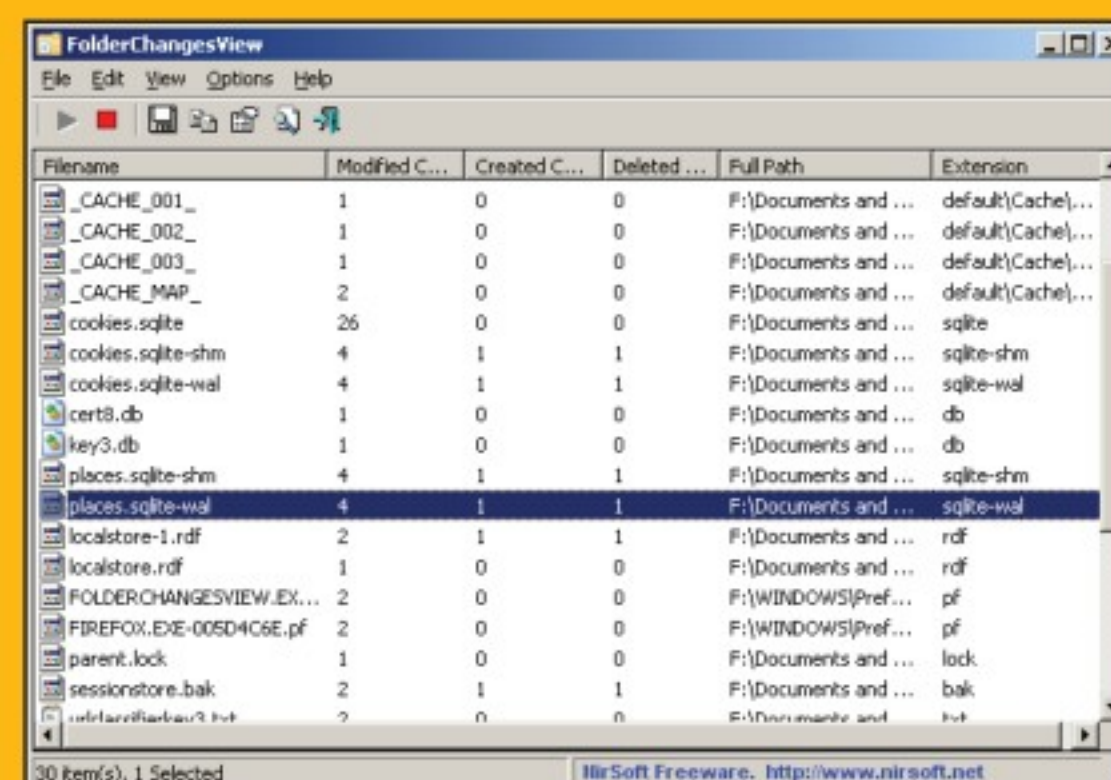


FOLDERCHANGESVIEW

> PORTABLE ET EN RÉSEAU

Déterminez quels fichiers ont été créés, modifiés ou supprimés avec FolderChangesView. Il analyse les disques de votre choix (en local ou en réseau) et se présente également en version portable, sans installation (une clé USB suffit pour l'utiliser). Cependant, p de Windows 10.

Lien : bit.ly/3ClrY0P



Casser les codes et décrypter l'info

JE M'ABONNE à PIRATE INFORMATIQUE

LIVRAISON
sous PLI
DISCRET

OFFRE ABONNEMENT



1 AN POUR 17 € (au lieu de ~~19,60 €~~)

2 ANS POUR 29,40 € (au lieu de ~~39,20 €~~)



LIVRÉ

CHEZ VOUS !



PRATIQUE &

ÉCONOMIQUE !



LES GUIDES du HACKER et du PIRATE

- > Logiciels et applications exclusifs
- > Tutoriels et astuces clairs
- > Dossiers pratiques complets pour débutants et experts
- > Sélection et test de matériels
- > L'actu et les nouveautés !

RÉDUCTION
DE
-25%



À DÉCOUPER (OU À PHOTOCOPIER), À COMPLÉTER ET À REnvoyer sous enveloppe affranchie à :
BII - SERVICE ABONNEMENT - 15, RUE DE MERY - 60420 MÉNÉVILLERS

- ☐ Abonnement à Pirate Informatique pour 4 numéros, je joins mon règlement de 17,00 €
- ☐ Abonnement à Pirate Informatique pour 8 numéros, je joins mon règlement de 29,40 €

☐ OUI, JE M'ABONNE :

Nom

Prénom

Adresse

Code Postal

Ville

E-Mail

☐ Je joins mon règlement par
chèque à l'ordre de ID PRESSE
(France uniquement)

Offre valable en France métropolitaine
uniquement.

POUR NOUS CONTACTER :
abonnement@idpresse.com



Offre valable jusqu'au 31 décembre 2021. Les délais
d'acheminement de La Poste varient selon les régions et
pays. Conformément à la loi Informatique et Libertés du
6/1/1978, vous disposez d'un droit d'accès et de rectification
quant aux informations vous concernant, que vous pouvez
exercer librement auprès de ID PRESSE - IMPASSE DE
L'ESPÉRON - VILLA MIRAMAR - 13960 SAUSSET LES PINS

Signature obligatoire :

LES AVANTAGES :

- > Jusqu'à -25 % sur le prix en kiosques
- > Ne manquez aucun numéro
- > Ne soyez plus une victime
- > Vos magazines livrés chez vous gratuitement

LES DOSSIERS DU **Pirate**

DES DOSSIERS
THÉMATIQUES
COMPLETS

À DÉCOUVRIR
EN KIOSQUES

PETIT FORMAT

MINI PRIX

CONCENTRÉ
D'ASTUCES



**VIE
PRIVÉE &
ANONYMAT**



Actuellement #Guide pratique

ANONYMAT

PROTECTION

ESPIONS

PODCASTS

RÉSEAUX SOCIAUX

BITCOIN

EMAILS

USB

SURVEILLANCE



PIRATE
INFORMATIQUE



BEL/LUX : 6 € - DOM : 6,10 € - CH : 8,50 ChF - PORT.CONT. : 6 € - CAN : 7,99 \$ cad -
POL/S : 750 CFP - NCAL/S : 950 CFP - MAR : 50 mad - TUN : 9,8 tnd